USDA United States Department of Agriculture
Departmental Administration

Information Technology Security

Procedure Guidelines

October 2004

TABLE OF CONTENTS

100 INTRODUCTION

101 PURPOSE

This Guide provides direction to Departmental Administration (DA) Program Offices as they develop procedures that make them fully compliant with the DA Information Technology Security (ITS) Program as described in the *DA Information Technology (IT) Security Policy Manual*. The procedures to be developed by each Program Office will assure that all DA information contained in DA IT systems is protected with regard to its availability, integrity, confidentiality, and continuity.

102 SCOPE

The guidance contained in the *DA Information Technology Security Procedures Guidelines* applies to the IT security procedures to be developed by all DA Staff Offices.

103 DA SYSTEM OPERATIONS

The procedures developed using these guidelines apply to the full life cycle of all systems development, portable and fixed hardware, software, firmware, media, and facilities used to support the DA mission. The life cycle includes, but is not limited to, all actions related to a system from its inception or procurement to its replacement, removal, and/or destruction. The procedures also apply to any changes to DA IT systems.

104 OTHER ORGANIZATIONS

The procedures developed using these guidelines apply to any outside organizations, including contractor organizations, or their representatives, who are granted access to DA's IT resources.

105 ROLES AND RESPONSIBILITIES

Each section in this guidance includes specific roles and responsibilities related to the procedure addressed. The roles and responsibilities described below are general and may be delegated unless otherwise noted.

105.1 Assistant Secretary for Administration

Has the overall responsibility to ensure that all DA information systems are protected commensurate with the risk to the systems and the information they contain. The DA security procedures developed consistent with the guidance provided here will be in accordance with all relevant federal laws, regulations, and USDA guidelines.

105.2 Designated Approving Authority (DAA)

The DAA is responsible for the security of information within his/her organization. The DAA must ensure the protection and continuity of organizational computer systems, networks, and data operations. The DAA has the authority to approve the procedures developed by DA program offices as consistent with both the guidance in this document and the policy promulgated in the DA Information Technology (IT) Security Policy Manual. The DAA for DA is the Assistant Secretary for Administration.

105.3 DA Chief Information Officer (CIO)

The CIO is responsible for developing DA ITS program procedures. The CIO will ensure that DA organizations appoint an individual Information Systems Security Officer (ISSO) for each of their DA IT functions. The detailed responsibilities and duties of these appointees will be found in the DA Information Technology Security Policy Manual. The CIO**:**

1. Ensures that DA security procedures and practices are in accordance with all relevant federal laws, regulations, and USDA guidelines.
2. Ensures development and implementation of procedures for the DA IT community are coordinated; and,
3. Ensures DA compliance with all relevant USDA and federal laws, regulations, and guidelines.
4. Ensures development and implementation of USDA required policies and procedures related to the approval, use, and access to DA IT systems using portable and remote access devices in accordance with USDA OCIO Memorandum CS-037, Information Technology Systems, Chapter 10, Part 4, Laptop and Portable Computer Security.
5. Establish procedures to fully complete the portable laptop and desktop computers checklist and the Telework and Remote Access Checklist contained in USDA Guidance CS-029

105.4 Office of Operations (OO)

The Office of Operations (OO) has responsibility for developing the security procedures for DA computer networks, telecommunications infrastructures, and for General Support Systems (GSSs) under its control.

105.5 DA Information System Security Program Manager (ISSPM)

The DA ISSPM is the internal DA IT security specialist responsible for coordinating, defining, and implementing security policies and procedures for the overall DA IT activities, including the coordination and management of the security aspects related to the use of PEDs, wireless and remote access devices, including laptop and desktop computers and peripherals used for remote access to DA systems. The ISSMP also:

1. Coordinate and manage the security control required for wireless and remote access devices, including laptop and desktop computers and their peripherals, used in remote access arrangements.

2. Assists DA managers in completing the appropriate checklists including those in USDA CIO, CS-029 Guidance, as required;

3. Coordinate and oversee the completion of the portable laptop and desktop computers checklist and the Telework and Remote Access Checklist contained in USDA Guidance CS-029.

4. Routinely monitors DA implementation of these devices to ensure that policy and procedures are followed;

5. Advises DA managers in cases of lax security controls or improper use;

6. Assist in developing waiver packages, as required;

7. Participate in the development of technology implementation plans;

8. Update the DA System Security Plan and other documents to reflect the funding and planned implementation of portable laptop and desktop computers used in remote access arrangements; and,

9. Develops the documentation guidance for the DA to delete or purge data on PEDs, wireless and remote access devices, including laptop and desktop computers and peripherals used for remote access to DA systems in cases of suspected compromise and oversees the implementation of that right.

105.6 Agency System and Network Administrators.

Agency System and Network Administrators are the IT professionals responsible for adhering to the DA Rules of Behavior and security requirements contained in their system's System Security Plans (SSPs). Generally, these professionals manage the activities of the servers and applications that drive the GSS and its MAs. As the use of technology expands and the ability to remotely access the GSS and its MAs from Telecommuting Centers, a user's home, or when a user is on travel status, remote access becomes more of an operational option. These professionals must ensure that the security of the systems and networks that administer remain secure in a remote access environment. To accomplish this that must:

1. Provide appropriate administrative access and permissions for these portable laptop and desktop computers used in remote access arrangements based job requirements;

2. Install encryption, VPN Technology and require strong authentication for these devices, especially in cases where Sensitive But Unclassified (SBU) information will be transmitted or stored;

3. Install standardized configurations, strict security features, profiles and disable modems;

4. Routinely patch and update portable laptop and desktop computers used in remote access arrangements and check devices for unauthorized software or copyrighted material; and

5. Verify appropriate security controls are in place using the appropriate checklist included in this guidance and those in Cyber Security Guidance Regarding Telework and Remote Access, as required.

105.7 Information System Security Officers (ISSOs)

The ISSO for each DA Staff Office is responsible for coordinating, defining, and implementing security policies and procedures for all General Support Systems and Major Applications in their offices.

105.8 DA Information Technology Professionals and End Users

IT professionals and end users of DA systems are responsible for adhering to the DA Rules of Behavior and security requirements contained in their system's System Security Plans (SSPs). Additional information related to the assignment of duties to fulfill the requirements of the DA ITS Program is found in the USDA Security Program Plan (SPP).

106 RECORDS AND REPORTS

All records and reports established by this guide and all other DA IT security-related documents will be developed and managed in accordance with current USDA and DA record and report requirements.

107 AUTHORITIES AND REFERENCES

All authorities and references used to determine the requirements for and development of this document are listed in Appendix A. In the event that the guidance in this document conflicts with USDA requirements and guidance, the USDA guidance will be followed.

108 TERMS, DEFINITIONS, AND ACRONYMS

Appendix B provides the terms and definitions used in this document. Appendix C contains acronyms used in this document.

200 MANAGEMENT CONTROLS

200.1 MANAGEMENT CONTROLS

Management Controls address management of the security aspects of the IT system and the management of risk for the system. Management controls include risk management, review of security controls, system life cycle controls, processing authorization controls, and system security plan controls. In addition to the control of use of the assets of the IT system, control must also consider the remote access to the system through the use of portable and remote access devices used for telecommuting and other purposes that include, but are not limited to, devices such as a:

1. Desktop Computer
2. Laptop Computer,
3. Home Computer,
4. Bluetooth Device,
5. Personal Digital Assistants (PDA),
6. Portable Electronic Device (PED) and Wireless Devices. (Generally PEDs include, but are not limited to, cell phones, pagers, text messaging devices (Blackberries), hand scanners, portable digital assistants, and voice recorders, and flash memory.), and,
7. Portable Storage Device. (Generally these include, but are not limited to, ZIP drives, floppy disks, compact and DVD disks, flash memory cards, etc.)

200.2 MANAGEMENT CONTROL PROCEDURES

Management controls procedures support DA System Security Policy (SSP). Procedural requirements and more detailed information for each program element are found below and in the USDA Security Program Plan and specific DA Information Technology Security (ITS) procedures.

201 INFORMATION SENSITIVITY

201.1 PURPOSE

A determination of information sensitivity is the basis for security planning for each GSS and MA. As a part of this determination, a Privacy Information Assessment (PIA), as specified by the OCS, will be conducted on all DA information systems.

201.2 Scope

All GSSs and MAs must have sensitivity analyses as the basis for security planning. Information sensitivity within each GSS or MA must be determined in order to develop and maintain the appropriate security procedures. The information sensitivity determination must address the following elements as appropriate: confidentiality, integrity, and availability.

201.3 Roles and Responsibilities

201.3.1 The CIO

The CIO is responsible for ensuring that the information sensitivity of each GSS and MA has been addressed according to established guidelines.

201.3.2 DA Staff Office Directors

DA Staff Office Directors are responsible for ensuring that information sensitivity has been determined for each GSS and MA under their control and that appropriate steps are taken to protect the integrity and use of the information once this determination is made.

201.4 Procedures

The information sensitivity determination must address Confidentiality, Integrity, and Availability. Section 3.7.2 of the *National Institute of Standards and Technology (NIST) Guidance for Developing Security Plans for Information Systems, Special Publication 800-18* provides good examples of each of the categories and levels of information sensitivity. The sensitivity analysis should be summarized in a general protection statement for the system. The analysis of the DA GSS and MAs must include the potential use of wireless, remote, or portable means to access them. These means include, but are not limited to, laptop and home computers, PDAs or PEDs, e-mail capable cell phones, portable storage drives and disks, and other similar devices.

201.4.1 Authorities

Any laws, regulations, or policies that establish specific requirements should be referenced in the discussion of sensitivity. In particular, Systems of Records, as defined in the Privacy Act, must be protected from unauthorized use or modification.

201.4.2 Privacy Impact Analysis

As part of the sensitivity analysis, a Privacy Impact Assessment (PIA) must be conducted to evaluate privacy vulnerabilities and risks, and their implications on information systems. The assessment will determine whether personally identifiable information resides on the system, and if so, what type. The type of personal information collected, used, and maintained will determine which privacy laws are invoked, if any. If privacy vulnerabilities are identified, the Plan of Action and Milestones (POA&M) must be updated and a Privacy Act Notice must be prepared.

201.4.3 Factors and Levels of Concern

Confidentiality, integrity, and availability factors for all GSSs and MAs must be determined. These factors are described in detail below. For each one of these elements, systems should be categorized by level of concern. These levels are designated high, medium, and lows. The *NIST Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, Special Publication 800-37* provides definitions of the levels of concern. They are reproduced here following the definitions below.

201.4.3.1 Confidentiality

Confidentiality is defined as the level of protection required for the type of information contained in the system. The following are examples of information with confidentiality considerations:

1. Confidential business information;
2. Proprietary procurement information;
3. Confidential DA or USDA information;
4. Confidential information belonging to other government information;
5. Enforcement confidential information;
6. FOIA-exempt information;
7. Privacy Act information; and
8. Embargoed budget information.

201.4.3.2 Integrity

Integrity is the extent to which the information contained in the system must be protected from unauthorized, unanticipated, or unintentional modification. In general, the greater the needs for reliability and accuracy of information, the higher the requirements are for integrity. An example might be data the public relies on such as census information, economic indicators, or unemployment data.

201.4.3.3 Availability

Availability establishes the need for the information or services to be available on a timely basis to meet mission requirements or to avoid substantial losses. Information in this category includes information that the public depends on for safety such as environmental quality data or service such as information on job training services.

NIST: TABLE 3.1 LEVELS OF CONCERN FOR SYSTEM CRITICALITY/SENSITIVITY

	LOW	MODERATE	HIGH
CONFIDENTIALITY SENSITIVE BUT UNCLASSIFIED (SBU) INFORMATION	The consequences of unauthorized disclosure or compromise of data or information in the system is **generally acceptable**. Loss of confidentiality could be expected to affect agency level interests and have some negative impact on mission accomplishment.	The consequences of unauthorized disclosure or compromise of data or information in the system is only **marginally acceptable**. Loss of confidentiality could be expected to adversely affect agency-level interests, degrade mission accomplishment, or create unsafe conditions that may result in injury or serious damage.	The consequences of unauthorized disclosure or compromise of data or information in the system is **unacceptable**. Loss of confidentiality could be expected to adversely affect national level interests, prevent mission accomplishment, or create unsafe conditions that may result in loss of life or other exceptionally grave damage.
CONFIDENTIALITY NATIONAL SECURITY INFORMATION (CLASSIFIED)	Not applicable.	Not applicable.	The consequences of unauthorized disclosure or compromise of data or information in the system is **unacceptable**. Loss of confidentiality could be expected to cause exceptionally grave damage, serious damage, or damage to the national security.
INTEGRITY	The consequences of corruption or unauthorized modification of data or information in the system is **generally acceptable**. Loss of integrity could be expected to affect agency level interests and have some negative impact on mission accomplishment.	The consequences of corruption or unauthorized modification of data or information in the system is only **marginally acceptable**. Loss of integrity could be expected to adversely affect agency-level interests, degrade mission accomplishment, or create unsafe conditions that may result in injury or serious damage.	The consequences of corruption or unauthorized modification of data or information in the system is **unacceptable**. Loss of integrity could be expected to adversely affect national level interests, prevent mission accomplishment, or create unsafe conditions that may result in loss of life or other exceptionally grave damage.
AVAILABILITY	The consequences of loss or disruption of access to system resources or to data or information in the system is **generally acceptable**. Loss of availability could be expected to affect agency level interests and have some negative impact on mission accomplishment.	The consequences of loss or disruption of access to system resources or to data or information in the system is only **marginally acceptable**. Loss of availability could be expected to adversely affect agency level interests, degrade mission accomplishment, or create unsafe conditions that may result in injury or serious damage.	The consequences of loss or disruption of access to system resources or to data or information in the system is **unacceptable**. Loss of availability could be expected to adversely affect national-level interests, prevent mission accomplishment, or create unsafe conditions that may result in loss of life or other exceptionally grave damage.

201.5 MANAGEMENT CONTROLS

Information sensitivity within each GSS or MA system must be determined in order to develop and maintain the appropriate security procedures. Information sensitivity analysis should be done during the early stages of the project life cycle. If the nature of the data or processing circumstances changes, including the ability to access the system remotely or through wireless, remote, portable, or other similar devices, the sensitivity levels should be reviewed and revised, as appropriate. The analysis is the basis for risk management and security planning for the system during its life cycle.

201.5.1 Sensitivity Analysis

Sensitivity analysis is required to support the following functions:

1. System design, implementation, and operation;
2. Internal and external auditing of system security measures; and
3. Management decisions regarding the reasonableness of security countermeasures.

202 RISK MANAGEMENT

202.1 Purpose

Risk management covers assessing the acceptable level of risk for a GSS or MA and determining appropriate safeguards. Risk management procedures have to be established for DA systems throughout their life cycles, including any changes or modifications to them. A risk analysis may also determine or limit the level and degrees of access allowed for the system through wireless, remote, or portable means, such as, laptop and home computers, PDAs or PEDs, e-mail capable cell phones, portable storage drives and disks, and other similar devices.

202.2 Scope

Each GSS and MA must have a risk analysis completed to ensure that it is protected at a level of risk that has been determined to be acceptable by management. Risk management procedures must be established that cover DA systems throughout their life cycles, including any changes or modifications to them.

202.3 Roles and Responsibilities

202.3.1 The CIO

The CIO is responsible for ensuring that:

1. Risk and Vulnerability Assessments of DA GSSs and MAs are conducted as required by the appropriate federal authorities; and

2. All threats to the effective operation of DA IT systems are communicated to DA divisions and staff offices and that appropriate actions are taken promptly to protect DA computer assets.
3. The risk to the GSS and MAs caused by allowing remote access by PED, laptops, and desktops computers for telecommuting or other purposes is included in the Risk and Vulnerability Assessments. Additionally, DA will risk assessments on these devices and complete the appropriate checklists in USDA OCIO Memorandum 037, Chapter 10, Part 4, Table1 to assess the security posture and countermeasures necessary to ensure all security requirements are satisfied

202.3.2 DA Staff Office Directors

DA Staff Office Directors are responsible for implementing risk management procedures and for ensuring that risk and vulnerability assessments are carried out for each GSS and MA under their control.

202.4 Procedures

Risk management consists of identifying, controlling, and mitigating information system-related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws. Findings developed in the initial assessment of information sensitivity should be used as a basis for the risk assessment.

202.4.1 Risk Assessment

The assessment must:

1. Consider mission criticality, data sensitivity, and data integrity;
2. Identify threat sources, both natural and manmade;
3. Determine and list the vulnerabilities, flaws, and weaknesses that identified threats may exploit;
4. Determine the potential risk involved in allowing access to the system through wireless, remote, or portable means, such as, laptop and home computers, PDAs or PEDs, e-mail capable cell phones, portable storage drives and disks, and other similar devices. .
5. Assess the degree of threat or harm to the system that exploitation could cause; and,
6. Analyze whether the security measures in place adequately mitigate the vulnerabilities.

202.4.2 Criticality and Vulnerability

Criticality and vulnerability assessments provide a way to determine that the level of acceptable risk for a GSS or MA is commensurate with the requirements of the system for confidentiality, integrity, and availability. Criticality and vulnerability findings are the basis for recommendations for risk reduction and budgetary, operational, and data restoration priorities. The DA Staff Office Directors, system managers, and the ISSO determine the vulnerability of each MA and GSS.

202.4.2.1 Criticality

The criticality of each MA and GSS is determined by assessing the three aspects of criticality: 1) confidentiality, 2) integrity, and 3) availability. These aspects are defined as follows:

1. **Confidentiality.** The system contains information that must be protected from unauthorized access.
2. **Integrity**. The system contains information that must be protected from unauthorized, unanticipated, or unintentional modification.
3. **Availability**. The system contains information or provides services that must be available on a timely basis to meet mission requirements or to avoid substantial losses.

202.4.2.2 Vulnerability

Vulnerability is defined as a flaw or weakness that may allow harm to occur to an automated information system or activity. Vulnerability assessment considers weaknesses relating to the platform, personnel, physical environment, and communications aspects of the MA or GSS, including access using wireless, remote, or portable means, such as, laptop and home computers, PDAs or PEDs, e-mail capable cell phones, portable storage drives and disks, and other similar devices. Known security problems, configuration errors, and the installation of hardware/software “patches” are also considered.

202.4.2.3 System Safeguards

Risk assessment must discuss safeguards utilized for the GSS or MA. These safeguards should cover platform, communications, personnel, and physical security as needed. Potential risks should be prioritized according to their likelihood of occurrence and impact. Safeguards should address each of the risks. The discussion should be consistent with sections of the SSP where these safeguards are addressed in more detail.

202.5 Management Controls

Risk assessments must be performed throughout the life cycle of each DA GSS and MA. They must be performed, at a minimum, every three (3) years; as a result of an adverse finding from a security controls review; or whenever significant changes are made to a system, its architecture, or any of its major applications.

203 SECURITY CONTROLS REVIEW

203.1 PURPOSE

A thorough and ongoing security controls review process is essential to ensure that DA adequately protects its information systems, software, and hardware from breaches. Further this review process establishes procedures for prompt corrective action of any weaknesses or security control incidents.

203.2 SCOPE

The DA security controls review procedures apply to all GSSs and MAs and to other DA systems interfacing with them.

203.3 ROLES AND RESPONSIBILITIES

203.3.1 Assistant Secretary for Administration

Assistant Secretary for Administration (or designee) assures that all security policy and procedures are consistent with federal law and regulation and that adequate budget/funding for security controls and reviews is available. The Assistant Secretary (or designee) transmits documentation on the results of the DA annual security controls review to the USDA OCIO.

203.3.2 The CIO

The CIO ensures that effective DA-wide security controls exist and that periodic reviews of all DA systems and any externally interconnected systems are conducted according to the guidance in *OMB Circular A-130*. The CIO must ensure that DA Staff Office Directors are informed of the results of the reviews, and that they address any deficiencies or weaknesses.

203.3.3 DA Staff Office Directors

DA Staff Office Directors are responsible for conducting internal security controls reviews on systems under their control, for cooperating with external security controls review teams, and for implementing any corrective actions that result from these reviews.

203.3.1 Information System Security Officers

Information System Security Officers (ISSOs) have responsibility for developing security controls procedures, scheduling internal reviews, and completing follow-up actions.

203.4 PROCEDURES

The security controls review procedures provide DA with the information needed to evaluate security controls. Any deficiencies found during these reviews are reported in the DA POA&M.

203.4.1 External Review Process

A security controls review must:

1. Cover management, operational, personnel, and technical controls;
2. Consider the security impact of allowing access using wireless, remote, or portable means, such as, laptop and home computers, PDAs or PEDs, e-mail capable cell phones, portable storage drives and disks, and other similar devices.
3. Be conducted independent of the manager responsible for the application; and
4. Be of a type and rigor commensurate with the acceptable level of risk for the system or the likelihood of learning useful information to improve security.
5. Ensure the reporting of any serious weaknesses as deficiencies in accordance with *OMB Circular No. A-123* and the Federal Managers' Financial Integrity Act.
6. Reviews initiated and conducted by the USDA Inspector General (IG) or the General Accounting Office (GAO) are considered to fulfill the external review requirement.

203.4.2 Internal Review and Evaluation

Internal DA reviews must be conducted annually, whether or not there has been an external review. They must include at a minimum:

1. A rigorous self-assessment process;
2. An examination of each operating system's configuration to ensure it can prevent circumvention of security software and application controls;
3. An analysis of security alerts and incidents, and the subsequent remedial actions; and,
4. Verification that key controls are examined and tested. For example, network scans, reviewing router and switch settings, and conducting penetration tests.

203.4.3 Ad Hoc Reviews

An informal review of security controls should be conducted as part of the investigation of any major security breach. If the breach involves a GSS, MAs utilizing that GSS should also conduct an informal security controls review. The most recent internal and/or external review should be examined to determine whether the security breach exploited known weaknesses or deficiencies and whether these weaknesses or deficiencies were in the process of being corrected. Any deficiencies found during these reviews should be documented in the appropriate DA POA&M.

203.5 MANAGEMENT CONTROLS

203.5.1 Corrective Action Plans

After every review that identified weaknesses or deficiencies in a GSS or MA, the Staff Office Director with responsibility for the system must develop a corrective action plan.

203.5.2 Security Controls Review Logs

A log must be maintained of all security controls reviews performed on GSSs and MAs. This log must incorporate the schedule for annual reviews and must note all non-scheduled reviews that take place during the year. The schedule log must document the timing of each review, the organization that performed the review, whether any weaknesses or deficiencies were identified, and whether a corrective action plan has been prepared.

204 RULES OF BEHAVIOR

204.1 PURPOSE

Rules of behavior are the rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. They are a form of security controls applied to system users with the intent of mitigating risks that could be inadvertently or intentionally imposed by those users. These rules clearly delineate the responsibilities and expected behavior of all individuals with access to a specific system. The rules must state the consequences of inappropriate behavior and the rules must be associated with technical controls implemented in the application. The rules should include, for example, limitations on changing data, searching databases, access using wireless, remote, or portable means of access or divulging information.

204.2 SCOPE

Rules of behavior are specific to each MA or GSS and must be consistent with administrative and technical security controls in these systems. The rules must be only as stringent as necessary to provide adequate security for the system and the information it contains. Rules must be included in the SSPs and made part of security and awareness training. Rules must also address interconnections to other systems and remote access using wireless, remote, or means, such as, laptop and home computers, PDAs or PEDs, e-mail capable cell phones, portable storage drives and disks, and other similar devices. Rules of behavior must be provided to each system user before that user is allowed access to a system. The Rules of Behavior apply to government contractors as well as to federal employees. As part of their rules of behavior, remote access users must be made aware of the DA "Personal Use Policy" and restrictions on the use of Private Internet Service Providers (ISP), specified user locations, the methods of access, the prohibitions on changing or disabling security features including encryption/decryption features on the devices and the use of unauthorized or copyrighted software and materials, and the use of non-USDA devices.

204.3 ROLES AND RESPONSIBILITIES

204.3.1 The CIO

The CIO is responsible for verifying that rules of behavior have been published and are being followed.

204.3.2 DA Staff Office directors

DA Staff Office Directors have overall management responsibility for the development and implementation of the rules of behavior for the GSSs and MAs under their control.

204.4 PROCEDURES

Rules of behavior must address responsibilities, expected behaviors, and penalties for inappropriate behaviors. Users must be notified of rules of behavior for any system to which they are being granted access.

204.4.1 Responsibilities.

The rules of behavior must define all individual roles with respect to a system and must describe the responsibilities of each individual (government employee and contractors).

204.4.2 Expected Behavior.

The rules of behavior must address all interactions with the system including limitations on modifying data, searching databases, or divulging information. They must address use of passwords, access limitations, and control of user workstations. For example, users must be advised if the rules of behavior dictate that workstations must not be left logged on for more than a prescribed period of time. As another example, users with access privileges must be told that system information can be used only to the extent required to do their jobs. They must also state whether the system may be accessed using wireless, remote, or portable means, such as, laptop and home computers, PDAs or PEDs, e-mail capable cell phones, portable storage drives and disks, and other similar devices.

204.4.3 Controls.

Rules of behavior must also include appropriate controls over employee-initiated interconnections with other systems and must define service provision and restoration priorities. Depending on the nature of the specific system, rules of behavior may be required to address:

1. Work at home,
2. Dial-in access,
3. Wireless Access,
4. The use of portable storage devices such as, ZIP Drives, floppy, CD, and DVD disks, flash memory cards, and other similar devices.
5. Unofficial use of government equipment,
6. Assignment and limitation of system privileges, and
7. Individual accountability.

204.4.4 Penalties.

Rules of behavior must include clear descriptions of penalties for inappropriate behavior. These penalties range from written reprimand to criminal prosecution. Users must be informed specifically of actions that would render them criminally liable. In this instance, the user must be told the extent of prosecution in terms of fines and imprisonment, or both. If actions would be subject to civil penalties, the user must be advised as to the potential extent. If user actions are subject to specific codes (e.g. Internal Revenue Code), users must be advised of those codes.

204.5 MANAGEMENT CONTROLS

204.5.1 Risk Assessment Use

The definition of rules of behavior for a specific system is based on an understanding of the risk involved in the compromise or corruption of information contained in that system. The system risk assessment should be completed and used as a guide to determine rules of behavior. As the risk assessment is updated and/or as a result of security controls review, the rules of behavior may require modification.

204.5.2 Distribution of Rules of Behavior

Rules of behavior must be provided to each system user before that user is allowed access to a system. The rules of behavior should be published. It is recommended that all users be required to sign them to acknowledge that these rules have been read. The system manager may require contractor personnel to sign system specific non-disclosure agreements.

205 LIFE CYCLE SECURITY MANAGEMENT

205.1 PURPOSE

Security concepts and practices must be included throughout an IT system's entire life cycle in order to ensure the protection of a system and its hardware, software, firmware and data.

205.2 SCOPE

The National Institute of Standards and Technology (NIST) uses a five-phase version of the life cycle. It describes the following phases of an IT project: Conceptual Planning, Planning and Requirements Definition, Design and Development, Implementation, Operations and Maintenance, and Disposition. The list of considerations below is based on these phases. For legacy systems, only the implementation, operation and maintenance, and disposition phases may be applicable in regard to system life cycle planning.

205.3 ROLES AND RESPONSIBILITIES

205.3.1 CIO

The CIO is responsible for ensuring that security management is addressed during the entire life cycle of all DA GSSs and MAs, including the management of the security of assets used to provide remote access to them.

205.3.2 DA staff Office Directors

DA Staff Office Directors are responsible for overseeing the development and maintenance of full life cycle security management for all GSSs and MAs, including the management of the security of assets used to provide remote access to them under their control. They approve security requirements and assure their implementation.

205.3.3 System Managers

System Managers are responsible for preparing and maintaining life cycle security documentation, validating security requirements are met, and assuring that any revisions to the GSS or MA result in reviews of security controls.

205.4 PROCEDURES

Strong configuration/change management and quality assurance management practices must support life cycle security requirements and include documentation as well as software artifacts.

For legacy systems, only the implementation, operation and maintenance, and disposition phases may be applicable in regard to system security life cycle planning.

205.4.1 Conceptual Planning and Requirements Definition

This phase encompasses determining and documenting the business case for the system. The business case is incorporated into the Capital Planning and Investment Control process as part of the project proposal. As such, it must be fully compliant with OMB Circular A-130 direction and must include the security resources required as part of the investment portfolio. It must also include a sensitivity assessment and a PIA must be completed. The sensitivity of the information to be processed and that of the system itself must be considered. The sensitivity assessment should consider information elements as both single entities and as elements in combination. This is important, for example, if Privacy Act data is being processed and stored. The Privacy Act prohibits information elements from being combined and used for purposes that are incompatible with their Privacy Act notifications. The PIA will greatly affect a decision as to whether to allow access to the system using wireless, remote, or portable access devices. If the PIA establishes that Privacy Act data will be collected, stored, processed, and accessed by the system, Federal Register Notice action must be completed. A template is available for completing the PIA.

205.4.2 Conceptual Planning Phase

The Conceptual Planning phase encompasses determining and documenting the business case for the system. The business case is incorporated into the Capital Planning and Investment Control process as part of the project proposal. It must be fully compliant with *OMB Circular A-130* and must include the cost estimates for establishing and maintaining life cycle security.

205.4.2.1 Plan of Action and Milestones

A DA Plan of Action and Milestones (POA&M) is initiated in this phase. The POA&M must contain a brief description of security weaknesses in the system and a plan for correcting them, along with the dates when the corrections will be made. Quarterly updates to the POA&M are required during the entire life of the system.

205.4.2.2 Risk Assessment

During this phase, the initial risk assessment is conducted to determine security requirements including those required for the use of PEDs, including laptop and desktop computers to access the GSS and its MAs. These requirements, which include technical features, assurances, and/or operational practices, should be developed as part of the overall system requirements. The risk assessment builds on the sensitivity analysis conducted in the Conceptual Planning phase and becomes the basis for development and implementation of all security features in the system.

205.4.2.3 Security

The System Security Plan (SSP) is initiated in this phase of the life cycle. Security controls are developed at this point so that they will be in place during the entire life cycle of the system, including during its initial phases. A template is available for both GSS and MA SSPs to assist with this requirement.

205.4.2.4 System Interconnectivity Agreements

Systems that are interconnected for the purpose of sharing sensitive information must have signed and approved Memorandums of Understanding/Agreements (MOU/A) in place before establishing the interconnection. All MAs must have MOU/As that cover the security requirements that will be met by the supporting GSS. The MOU/A must specifically state whether either involved system can be accessed by wireless, remote, or portable devices and specify the type of device(s) and provide information related to the security configuration requirements needed to allow sufficiently secure remote access. The MOU/As must attest to the acceptance of the countermeasures in the system and the residual risk inherent in the system's implementation. These MOU/As must be accepted and signed by the responsible program officials.

205.4.2.5 Procurement and Security Requirements

The procurement documents should address the need to maintain a level of security controls through regularly scheduled system upgrades for computers directly attached to the GSS or its MAs, as well as PEDs, including laptop and desktop computers and their peripherals that are allowed to access them remotely. The documents guiding the procurements of these items must meet local functionality and performance standards to include, as a minimum, CPU operating speed, RAM and storage memory sizes, authorized operating systems, and authorized peripherals. The documents should address the ability to upgrade security controls as new threats and vulnerabilities are identified, and to incorporate new security technologies. If security requirements are critical, it may be necessary to include a demonstration during the procurement process to verify security capabilities. Procurement documents for commercial or off-the-shelf applications should identify and include system security requirements as part of the specifications. This would include requirements such as multi-level access control, audit trails, password implementations, and other technical controls.

205.4.3 Design and Development Phase

The Design and development Phase includes, but is not limited to, the following actions:

1. The objective of contingency planning is to ensure that systems are able to recover from processing disruptions caused by localized emergencies and large-scale disasters. A Contingency-Disaster Recovery Plan (C-DRP) is developed in this phase to address localized security incidents. These include emergency response capability that ensures that reasonable continuity of support is provided if events occur that prohibit normal operations. Each MA must have system-specific information developed for its disaster

recovery requirements, which are then coordinated with GSS management and added to the GSS C-DRP.

2. Rules of behavior, for all individuals with access to the system, including those relating to the use of remote access devices, are developed during the System Design Phase, and are modified as necessary in subsequent life cycle phases.

3. Separation of Duties should also be considered during the System Design phase. Based on the level of risk inherent in the system, the need for separation should be a recognized part of the design.

4. Security controls are tested to uncover any design flaws that would violate security policy. Security Test and Evaluation (ST&E) may be conducted as part of system testing. ST&E involves verifying that a system's security mechanisms are adequate, complete, and correct, and that the system documentation is consistent with actual operations.

5. The Risk Assessment (RA) is completed in this phase and added to the Certification package.

6. A preliminary Certification Package consisting of the SSP, RA, ST&E, and a Certification Statement is completed and submitted to the CIO for review and approval.

7. A Training Plan is constructed that addresses security concerns including instructions on how to utilize security features and appropriate rules of behavior for the system. Security considerations should be incorporated into the Training Plans for system administrators as well as end users.

205.4.4 Implementation Phase

The Implementation Phase includes, but is not limited to, the following actions:

1. Security requirements should undergo a design review and should be validated for compliance by system test. Security features and controls should be configured and enabled for the system. These features and controls should be installed and tested.

2. Design reviews and system security tests must be completed and documented prior to system implementation. The security documentation should be maintained in the official organization records. Documentation should indicate when and by whom the testing was performed. Once successful testing has been completed, the system should be authorized for processing. No DA system will be implemented prior to receiving written authorization to do so.

3. If the system is being implemented in an incremental fashion, security tests may be conducted on each portion of the system. In this case, information on the scope, time, and responsible party must be maintained. Once the entire system is completed, it must be further tested to ensure that all of the security requirements have been met.

4. Whenever DA IT system's security controls are modified or the system features are altered, the security controls must be tested and modified as necessary.

5. A final Certification package is completed and forwarded to the CIO for approval. No DA system will be implemented prior to receiving written authorization to do so.

6. All final security documents are posted to OMB data base as required.

205.4.5 Operation and Maintenance Phase

The Operation and Maintenance Phase includes, but is not limited to, the following actions:

205.4.5.1 Operations.

1. Operations of a system refer to the day-to-day functioning of the system. During this phase, activities include security operations and administration, operational assurance, and audits/monitoring.

2. Security operations include functions such as training, system backups, user administration and access privileges, and cryptographic key management. These functions should be described in system documentation and their use should be verified.

3. Operational assurance involves validating system operation against current security requirements, and covers personnel and technical controls. A definition of system features and the roles and responsibilities of managers, administrators, and users of the system should be documented.

4. Audits are generally one-time events where any or all security features of a system may be tested. Audits may be external or internal. If internal, audit procedures and schedules should be developed by the system managers. Monitoring refers to a real-time review of system activities (such as keystroke monitoring). System functions should support monitoring and procedures and should be in place that describe the monitoring process.

205.4.5.2 Maintenance

1. During their life cycle, most systems undergo modifications. These modifications may range from simple fixes (changes to tables or dates) to more complex modifications that imply redevelopment and potentially a new acquisition cycle.

2. A procedure should be established to test the impact of simple fixes and verify that security requirements continue to be met. The nature of the fix, the tests conducted, and the results should be documented in DA Configuration Management Plan.

3. Complex changes requiring new development and/or acquisition may include changes such as data base migration or conversion to web enabled information extraction and dissemination. A complex change requires a re-evaluation of both system and security requirements and a re-initiation of the development and acquisition phases. Security documentation should be revised to include any changes and each change should be retested and validated. Documentation on tests conducted, times, responsible parties, and results should be maintained.

5. During this phase the SSP is reviewed annually to assure that it remains current. Whenever system's security controls are modified, the security controls are tested, and the system is re-certified and re-accredited.

205.4.6 Disposition

205.4.6.1 Disposition of Information

In this phase the system is being abolished. The information contained within the system is either being converted to a new system, archived according to prevailing regulations, or destroyed. Certain system information such as passwords and cryptographic keys may require special disposal procedures. If archived information will be accessed in the future, measures must be taken to ensure its security. Information that is to be destroyed requires selection of methods appropriate to the nature of the information. Procedures for disposal of information should be described in the SSP and standard operating procedures. The procedures must include the disposition of wireless, remote, or portable means, such as, USDA issued laptop and home computers, PDAs or PEDs, e-mail capable cell phones, portable storage drives and disks, and other similar devices that can access the system.

205.4.6.2 Disposition of Hardware

The hardware that supported the system is generally a candidate for disposal as well. Information on removable media may be cleared or purged. The former renders it inaccessible by keyboard attack; the latter renders it inaccessible under laboratory attack. Three acceptable methods of purging are overwriting, degaussing, and destruction. The method selected should be the one that most fully meets the risk requirements of the information. Wireless, remote, or portable means, such as, USDA issued laptop and home computers, PDAs or PEDs, e-mail capable cell phones, portable storage drives and disks, and other similar devices must be subject to the same hardware disposition procedures as fixed hardware.

205.5 MANAGEMENT CONTROLS

205.5.1 Security Considerations

Life cycle security considerations are based on the risk assessment initially conducted for the system. Security requirements resulting from the risk assessment should be implemented, maintained, and tracked throughout the system life cycle. Managers should ensure that security requirements are integrated into their systems from the initial phase and that these requirements are documented. Security documentation should be kept current during the entire system life cycle.

205.5.2 System Security Plan

Processes adapted for life cycle security should be described in the SSP. These processes should be coordinated with configuration management, certification and accreditation, and other key system management processes.

206 CONFIGURATION/CHANGE MANAGEMENT

206.1 PURPOSE

Configuration/change management establishes uniform practices for changes made to hardware and software during the life of a GSS or MA. These changes are developed, tested, approved, and tracked according to a configuration/change management plan. The plan assures that there is discipline and accountability for changes made. This discipline will assure that changes do not initiate security breaches in formerly certified systems.

206.2 SCOPE

A configuration/change management plan must be developed and maintained throughout the system life cycle for all DA GSSs and MAs. The configuration/change management plan must ensure that all system changes are tested, documented, and approved.

206.3 ROLES AND RESPONSIBILITIES

206.3.1 CIO

The CIO is responsible for issuing guidance on configuration/change management plans and ensuring that each GSS and MA has such a plan in existence. This includes developing standard configuration for, and ensuring the continuous appropriateness of the configuration of, the Operating System software, firmware and authorized applications used in wireless and remote access devices and peripherals authorized to access the GSS and its MAs.

206.3.1 DA Staff Office Directors

DA Staff Office Directors are responsible for establishing and maintaining a configuration/change management process (documented in a configuration/change management plan) for GSSs and MAs under their control.

206.4 PROCEDURES

Configuration management is a family of security controls in the management class dealing with the control of changes made to hardware including wireless, remote, or portable devices, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an IT system.

206.4.1 Configuration of Wireless and Remote Access Items

206.4.1.1 General

To ensure appropriate use of wireless and remote access items, PEDs, laptop and desktop computers, peripherals, and modem software will be configured to restrict the user to the official job requirements of the person issued the item(s). Wireless and remote access devices, including laptop and desktop computers, will be properly configured for data synchronization. Users are prohibited from making any changes to the configuration of the DA issued wireless or remote access device, including laptop or desktop computers.

206.4.1.2 Multiple Users

Wireless and remote access devices, including laptop and desktop computers, checked out for use by a multiple number of personnel must have individual profiles for each user. The individual profiles must be configured for each individual's needs and access rights. Multiple accounts are not permitted where equipment is assigned to a specific user.

206.4.2 System Modification

No DA GSS or MA will be modified unless the modification process is consistent with the configuration/change management process for that system. This applies throughout the full life cycle. It includes original system development, installation, and operation whether developed for DA use or obtained off-the-shelf. It also applies to any modification occurring during the operation and maintenance phase of the life cycle.

206.4.3 NIST Guidance

NIST 800-18 provides detailed guidance covering the hardware and software controls. This guidance should be the basis for configuration/change management procedures for each GSS and MA. Guidelines for development of configuration/change management plans are addressed in *Interim Guidance on USDA Configuration Management, CS-009.* Additionally, NIST 800-46, Security for Telecommuting and Broadband Communications provides guidance covering remote access devices and should be the basis for the management of secure access to the GSS and its MAs.

206.5 MANAGEMENT CONTROLS

Configuration/change management should be a formal process described in the SSP for each GSS and MA. This assures that all changes to a GSS or MA are reviewed and approved prior to implementation.

207 CERTIFICATION AND ACCREDITATION

The Certification and Accreditation (C&A) process provides assurance of the security of the system. It also establishes the level of risk that a senior manager is willing to accept in the operation of an IT system. All GSSs and MAs must be certified and accredited using the *OCIO OCS Certification and Accreditation Procedures.*

207.1 PURPOSE

The Certification and Accreditation (C&A) process provides assurance of the security of the system. It also establishes the level of risk that a senior manager is willing to accept in the operation of an IT system. All GSSs and MAs must be certified and accredited using the *USDA OCIO Certification and Accreditation (C&A) Guidance* provided on the OCIO intranet. The C&A package constitutes a living document that represents the formal agreement between the DAA, CO, program manager, and user representative.

207.2 SCOPE

Each GSS and MA must be formally accredited. Accreditation is based on complete documentation on all of system security procedures and safeguards, covering the total system life cycle. Accreditation may be full or conditional.

207.3 ROLES AND RESPONSIBILITIES

207.3.1 Assistant Secretary for Administration

The Assistant Secretary for Administration**,** or designee**,** is the Designated Approving Authority (DAA) for accrediting all DA IT systems in accordance with USDA OCIO OCS and DA policies and procedures. Acting on the advice of the Certifying Official, the DAA can accredit a system, issue an accreditation with conditions, issue a Temporary Authority to Operate (TAO), terminate a system's operation, or not permit a system to be placed in production.

207.3.2 CIO

The CIO is the Certifying Official (CO) for all DA IT systems. The CIO will ensure that the USDA Certification and Accreditation Process is employed for all DA GSSs and MAs and that the C&A process is carried out in accordance with the approved schedules provided by each ISSO. The CIO's office maintains a comprehensive inventory of all DA GSSs and MAs. When the CIO is designated to act as the DAA, this authority cannot be delegated.

207.3.3 Information System Security Program Manager

The Information System Security Program Manager **(ISSPM)** maintains an inventory of all GSSs and MAs.

207.3.4 Information Systems Security Officers

Information Systems Security Officers (ISSOs) are responsible for developing and maintaining all documentation and for preparing the SSAA for each GSS and MA under their control.

207.4 PROCEDURES

207.4.1 The C&A Package

The C&A package is developed during the Definition Phase of the System Development Life Cycle and is updated during each phase as new information becomes available.

207.4.2 Certifying Official's Evaluations

The CO evaluates the certification findings and assesses the vulnerabilities and residual risks associated with each GSS and MA. Based on the adequacy of system safeguards described in the C&A documentation, the CO recommends to the DAA that the DAA accredit a system, issue an interim authority to operate (IATO), terminate a system's operation, or not permit a system to be placed in production. If an IATO is issued, the C&A documentation must include corrective actions, a statement of residual risks, and an end date for the interim certification. The C&A documentation must provide a clear statement as to whether access by wireless, remote, or portable devices is allowed and, if allowed, the level of restriction on that access.

207.4.3 GSS and MA Requirements

Each GSS and MA must be formally accredited in accordance with USDA Guidance prior to system implementation, whenever major changes are made to the GSS or MA, and should be re-accredited once every three years.

207.4.4 System Inventories

An up-to-date inventory of systems (both developmental and operational), the anticipated dates for the C&A of developmental systems, the dates of the latest C&A for each operational system, and the projected dates for the next C&A of operational systems must be maintained. Reasons for changes to the C&A of any operational system must be reported to the CIO. The CIO must approve Certification and Accreditation schedules.

207.5 MANAGEMENT CONTROLS

For systems granted accreditation, full or conditional, the DAA's decision is based on the adequacy of system safeguards as described in the C&A package, compliance with USDA and DA IT guidance governing the system development life cycle, the vulnerability and risk assessment and security controls review processes for the system. The CIO, as the CO, ensures that the Program Office and the User Representative sign the C&A package after an affirmative review.

208 SYSTEM SECURITY PLAN

208.1 PURPOSE

The SSP describes the current controls and any planned controls for the system. It also delineates the security responsibilities of all persons having access to the system and defines their expected behavior when accessing the system.

208.2 SCOPE

SSPs are required for all GSSs and MAs. SSPs for other applications are not required because the security controls for those applications or systems would be provided by the GSSs within which they operate.

208.3 ROLES AND RESPONSIBILITIES

208.3.1 CIO

The CIO will provide guidance and ensure that SSPs are developed for all DA GSSs and MAs. The CIO must approve each SSP.

208.3.2 DA Staff Office Directors

DA Staff Office Directors are responsible for establishing and maintaining an SSP for all GSSs and MAs under their control.

208.3.3 Information System Security Program Manager (ISSPM)

The ISSPM for DA will provide guidance for and oversee the production of the SSPs for each DA system.

208.3.3 Information System Security Officers

The ISSO for each GSS and MA will develop an SSP for the system(s) for which he/she is responsible.

208.4 PROCEDURES

SSPs will include the procedures that implement DA IT security policies to ensure the integrity, availability, confidentiality, and continuity of the information contained in the IT systems. The SSPs will be developed in accordance with the guidelines set forth in the appropriate federal guidelines. (See Appendix A, Authorities and References). All SSPs will be developed using the template provided by the CIO. Each SSP will be updated annually or when current operating conditions or the risks to IT system operations change. A summary of the plan will be included in DA IT strategic planning documents as necessary.

208.5 MANAGEMENT CONTROLS

The CIO will review and verify the plans include procedures that implement the policies contained herein and ensure the integrity, availability, confidentiality, and continuity of the information contained in DA IT systems.

300 OPERATIONAL CONTROLS

Operational Controls address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems). Operational security controls include:

1. Preventive, e.g., control data media access and disposal; limit data distribution; control viruses; provide physical safeguards; guard wiring closets; conduct backups; use off-site storage; protect computing assets; guard against fire damage; provide emergency power source; and control heat and humidity of computing facility.

2. Detection, e.g., developing methods to determine the unauthorized access to and/or the misuse of data or equipment in any GSS or MA

301 PERSONNEL SECURITY

301.1 PURPOSE

Effective personnel security procedures are necessary to protect DA Information Technology (IT) systems from internal attack or misuse by persons having access to them.

301.2 Scope

310.2.1 Applicability

The personnel security procedures in this document apply to all DA employees and contract personnel performing work on, or accessing, DA IT systems. Personnel security procedures must be established within each DA Staff Office to ensure minimum compliance with current federal IT security standards.

301.2.2 DA Managers

DA managers must use this guidance in establishing the IT Personnel Security procedures for their organizations. DA procurement personnel can use this guidance to assure that appropriate personnel security specifications are included in DA IT acquisitions. The USDA Office of Human Resources and Management shall assist DA in implementing the procedures below.

301.3 ROLES AND RESPONSIBILITIES

301.3.1 CIO

The CIO approves all personnel security procedures related to the protection of any DA IT GSS or MA; approves requests for permission for individuals to access sensitive data prior to completion of a background check; and establishes DA process for requesting, establishing, and issuing IT user accounts. The CIO ensures mechanisms are developed and implemented by DA and the Office of Human Resources to hold users of DA IT systems responsible for their actions. The CIO also ensures mechanisms are developed and implemented by DA and IT procurement personnel to hold contract employees using any DA GSS or MA responsible for their actions. To ensure the appropriate use of DA issued wireless, remote access, including laptop and desktop computers and their peripherals, portable, or similar devices, the CIO, in coordination with the Office of Human Resources, will develop a "Personal Use Policy" applicable to DA as a whole related to those devices.

301.3.2 DA Staff Office Directors

DA Staff Office Directors establish personnel security procedures, consistent with DA and USDA policy, for GSSs or MAs under their control; and assure these personnel security procedures are kept current and implemented. Staff Office Directors approve requests for permission for individuals to access non-sensitive data on a GSS or MA under their control prior to completion of a background check and ensure a uniform DA process for requesting, establishing, and issuing IT user accounts is followed. Staff Office Directors also develop and implement mechanisms for DA and IT procurement personnel to hold contract employees using any DA GSS or MA responsible for their actions. Additionally, Staff Office Directors should ensure that the Employee Exit Procedures, DA-400-1 are followed for access to the IT user accounts.

301.3.3 Information System Security Officers

Information System Security Officer (ISSO) is responsible for writing, coordinating, and implementing personnel security procedures for the GSS and/or MAs controlled by her/his office; ensuring compliance with DA transfer and termination policies; and concurrently reporting any violation of personnel security procedures to the appropriate Staff Office Directors and the CIO.

301.4 PROCEDURES

The procedures developed for each DA GSS and/or MA must include the ability to hold persons accountable for their actions, and maintain the concept of "Least Privilege," and the separation of duties. The use of this guidance will ensure that all DA personnel, contractors, and system users understand the reasons for, and the intent of, the personnel security procedures. The following are specific personnel security procedural requirements:

301.4.1 Position Descriptions (PDs) and Hiring Requirements for Federal Employees

All position descriptions and hiring requirements for current or potential DA employees must:

1. Determine the sensitivity of the employee interfacing with a DA IT system in accordance with the sensitivity level assigned to the system;
2. Accurately reflect the system-related duties of the position in the PDs;
3. Separate the duties of the Systems Administrator and the ISSO in separate and distinct PDs;
4. Ensure the duty of administering access control functions will not be performed by the position that is responsible for administering access control audit trails;
5. Segregate the duties of employees using IT systems. For example, persons who enter financial data related to the payment of accounts must not be allowed to access system functions dealing with the establishment of accounts or placing orders against those accounts;
6. Divide the functions related to developing, testing, implementing, and maintaining data systems among different individuals;
7. Ensure all employees and contract personnel must obtain the appropriate level of clearance as defined by OPM and USDA personnel policies, before accessing DA IT systems or applications;
8. Ensure no DA employee will access an DA IT system before receiving initial security and awareness training in accordance with DA IT Security Policy;
9. Ensure Conditions of Employment will be established and enforced to ensure that appropriate action is taken in case of a violation of a security policy or procedure; and,
10. Ensure the USDA Employee Exit Procedures, DA-400-1 are followed for access to the DA IT user accounts.

301.4.2 Post Hiring Requirements for Federal Employees

After hiring an employee, Supervisors and managers must take the following actions.

1. Offices will adhere to the procedure established by the CIO for establishing, issuing, and closing user accounts for all DA IT systems;
2. No DA employee will be granted access to an DA IT system before receiving a background check (see exception request below);
3. Written justification for allowing an individual to access a DA GSS or MA when a background check has not been completed must be submitted to the CIO for approval. These requests must be limited to a specific period of time that cannot exceed the time required to carry out the necessary work or to complete the background investigation;
4. Offices will follow the procedures established by the CIO in conjunction with the Office of Human Resources to hold users responsible for their actions;
5. All DA Staff Office Directors will ensure that only persons granted an appropriate clearance will replace an individual who is sick, on vacation, on temporary duty or

assignment, or rotating to a different work shift. The assignment of these replacements may not violate the separation of duties requirements stated in DA SSP;

6. All program/regional administrators will ensure that only persons who are authorized access to the appropriate level of information sensitivity replace an individual who is sick, on vacation, on temporary duty or assignment, or rotating to a different work shift. The assignment of these replacements may not violate separation of duties requirements.
7. DA Employees are to be informed whether the system may be accessed remotely and whether the use of wireless, remote, or portable devices is allowed. Those employees allowed remote access will be informed of the access devices authorized for use, the way the system is to be accessed and the conditions placed on them and the use of the device(s).
8. When an employee is transferred or terminated, DA Staff Office Directors will use procedures and practices that protect the availability, integrity, and confidentiality of the data previously accessible to that employee including the retrieval of DA issued wireless, remote, or portable devices;
9. A uniform procedure must be established for closing user accounts after the user leaves a position or no longer needs access to the GSS or MA. This must occur no later than close of business the first business day after notification is received. This procedure must be monitored and follow the USDA Employee Exit Procedures, DA-400-1 for access to DA user accounts;
10. DA employees should complete appropriate Confidentiality or Security Agreements prior to being allowed access to the GSS and MAs they will be authorized to use. The restrictions in the agreement must be based on the sensitivity level of the GSS and/or MA they will access and the position they will fill; and,
11. All access controls relating to a particular employee will be appropriately changed or deleted immediately upon the termination or transfer of that employee and follow the USDA Employee Exit Procedures, DA-400-1 for access to DA user accounts.

301.4.3 Contractor Personnel

The following actions must be taken with regard to the issuance of contracts and the use of contractor employees.

1. Offices will assure that all contracts awarded on their behalf contain language that addresses security policy and procedures that apply to contract personnel and are commensurate with the sensitivity level of the GSS or MA accessed by contractor personnel;
2. Contract personnel must have the appropriate background check in accordance with USDA requirements before allowing them access to DA IT systems and information;
3. Written justification for allowing a contract employee to access a DA GSS or MA when a background investigation has not been completed must be submitted to the CIO for approval. These requests must be limited to a specific period of time that

cannot exceed the time required to carry out the necessary work or to complete the background investigation;

4. Procedures must be established that protect the availability, integrity, and confidentiality of sensitive data when contract personnel leave a project;
5. Contractor personnel are to be informed whether the system may be accessed remotely and whether the use of wireless, remote, or portable devices is allowed. If remote access is allowed, the employee will be informed of the access devices authorized for use, the way the system is to be accessed, and the conditions on the use of the device(s).
6. All access controls relating to a particular contract employee will be appropriately changed or deleted immediately upon his/her departure; and
7. Contract employees should complete appropriate Confidentiality or Security Agreements prior to being allowed access to the GSSs and MAs they will be authorized to use. The restrictions in the agreement must be based on the sensitivity level of the GSS and/or MA they will access and the function they perform.

301.4.4 Least Privilege Concept

Personnel access privileges are based on the "Least Privilege" concept. This means that a person is allowed to access a GSS or MA only to the minimum degree necessary to perform his or her job. Least Privilege means that restrictions are placed on the parts of the system to be accessed (e.g., access to data files, processing capability, or peripherals) and the type of access permitted (e.g., read only, read and write, execute, delete, etc.) The ISSO should be able to verify users and their level of privilege, including those allowed remote access to the GSS and/or its MAs.

301.4.5 Documentation

Personnel security procedures may be in a separate document or may be part of the SSP(s) for the system(s).

301.4.6 Coordination

Personnel security procedures must be coordinated with the head of a supported office when the procedures apply to GSSs or MAs used by another DA entity.

301.4.7 Reviews

Personnel security procedures must be reviewed annually. All deficiencies discovered during these reviews must be corrected.

301.5 MANAGEMENT CONTROLS

301.5.1 Personnel Security Training

DA Staff Office Directors must provide appropriate training to all employees so they can comply with and carry out the activities contained in the DA personnel security procedures.

301.5.1.1 Managers

This training must include any specialized training required for persons responsible for developing and overseeing the compliance with and use of personnel security procedures as part of their duties.

301.5.1.2 IT Security Personnel

Any DA employees designated ITSA, ITSO, or ISSO for their office or system must undergo training related to the types of personnel security problems related to IT systems, the methods and techniques used to circumvent IT personnel security measures, and the ways to prevent that circumvention. Each ISSO must also receive training on the requirements of specific personnel security procedures needed to protect the DA IT GSSs or MAs for which they are responsible.

301.5.1.3 System Users

System users at all organizational levels of DA must receive training on the personnel security procedures related to DA IT systems in general and specifically for the systems(s) supporting their operations. Appropriate levels of training will, at a minimum, familiarize them with personnel security procedures and the reasons why the procedures must be strictly followed. Personnel security information must be a part of the security training for all DA users.

302 PHYSICAL AND ENVIRONMENTAL SECURITY

302.1 PURPOSE

The *DA IT Security Policy Instruction* establishes the minimum requirements for the physical and environmental security of DA IT systems. These requirements are intended to ensure the availability, integrity, continuity, and confidentiality of the information contained in DA's GSSs and MAs.

302.2 SCOPE

Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. Physical and environmental security procedures apply to all software, firmware, hardware, data storage media, communications capabilities, and operational and storage facilities. Additionally, these procedures must cover physical access, adequate fire prevention, and continuous utilities support to the facilities. The provision of adequate physical and environmental security to the DA's GSS and MA operations and facilities is also dependent on the policies established in the *DA IT Security Policy Instruction*.

302.3 Roles and Responsibilities

302.3.1 CIO

The CIO is responsible for:

1. Ensuring that the physical and environmental security measures for all GSS and MA software, firmware, hardware, data storage media, communications capabilities, and operational and storage facilities are appropriately established and documented;
2. Ensuring that funds are requested to support the provision of physical access control, facility fire protection, continuous utilities support, and preventing the interception or unauthorized use of DA data;
3. Providing liaison support with USDA, the General Services Administration (GSA) and GSA's Federal Protective Service to obtain appropriate physical and environmental security support in facilities housing DA GSS and MA operations; and
4. Participating in the annual review of the IT security policy and procedures for each DA GSS and MA.
5. Ensuring that secure PEDs, including laptop and desktop computers, and their secure connectivity are used to remotely access the GSS and its MAs whether for telecommuting or other authorizes purposes. This includes strict physical accountability, developing standard configuration, using appropriate encryption, authorization, and Virtual Private Network (VPN) technologies, and establishing a formal waiver system for the use of PEDs, laptops and desktops, and authorized peripherals, that do not comply with USDA policy and approving waivers for their use.

302.3.2 DA Staff Office Directors

DA Staff Office Directors are responsible for: (1) establishing, following, and maintaining the procedures and records related to the physical and environmental security activities for their locations containing the GSSs and MAs under their control; and (2) coordinating with the providers of infrastructure services to ensure those not under DA control will not have an adverse impact on DA operations.

302.4 Procedures

Physical security and environmental security covers 4 areas: 1) Physical access control; 2) Fire safety; 3) Infrastructure support; and, 4) Wireless, remote, or portable systems.

302.4.1 Physical Access Control

Physical Access Control is applied to facilities operated by non-DA entities, facilities operated by DA or its organizational elements, and GSS or MA facility or library access.

302.4.2 Non-DA Facilities

When DA GSS and/or MA operations are housed in a building that has a primary federal occupant other than DA, the DA element is subject to the general building access controls of the primary occupant. Any additional physical and environmental security controls required by DA must be provided by DA.

302.4.3 Facilities operated by DA or its organizational elements.

When DA GSS and/or MA operations are housed in a building or room(s) primarily occupied by DA or one of its elements, the DA may establish additional physical access control procedures beyond those provided. Any procedures requiring alteration to the building or room must be coordinated with the appropriate federal building manager.

302.4.4 GSS or MA Facility or Tape/Media Library Access

To adequately safeguard the physical access to a data facility the following should be considered:

1. Restricting access to the facility to authorized personnel.
2. Permitting only authorized persons to access the tape/media library.
3. Assuring that entry to and exit from the facility is controlled by a positive means such as: picture Identification (ID) Card; security guard, key card; or biometric identification system.
4. Recording the issuance of appropriate entry identification/media showing the person’s full name, organization, date of issue, and, if appropriate, level of access in an issuance log.
5. Assuring that entry to and exit from a GSS or MA operating facility is recorded, either by using a log or, automatically by an automated system. If the facility is a tape/media library, the record must fully identify any items deposited to or withdrawn from it.
6. Maintaining a visitors' log that records name, time of entry, reason for visit, and time of exit. This log should also include the name of the person escorting the visitor. Each visitor should be issued an identification badge and be required to return it upon exit from the building. Visitors must be escorted while they are within the GSS or MA facility. The escort should initial the exit time of the escorted person in the visitors' log.
7. Reviewing the entry and visitor logs monthly to ensure that log entries are appropriately completed and to determine the legitimacy of the entry.

8. Requiring that documents showing approval for the issuance of the ID are on file and that the issuance remains valid.

302.4.5 Key Control.

Several methods can be used to open entryways to and exits from a data facility/room or tape/media library - mechanical keys, cipher locks, electronic key cards, and biometrics systems for instance. Key control procedures should address the following:

1. Only persons authorized in writing are provided keys that allow access to the system's facility or library. The authorization must be restricted to those normally working in the room/facility.
2. If regular mechanical locks are used, a log of those receiving the keys showing the person's full name, organization, date of issue, and return should be maintained.
3. Any logs kept that show individual PIN numbers or access codes used in conjunction with electronic entry/exit media should be maintained in a secured location.
4. Cipher lock codes, personal identification numbers (PINs), and/or access codes should be changed every quarter.
5. Any unused mechanical or electronic keys should be securely stored in a locked cabinet. Two persons must inventory unused keys simultaneously each month. To facilitate this inventory each key should have a distinctive number to identify it.
6. If a person leaves and the key is not returned then establish procedures to re-key the door for authorized persons.

302.4.6 Emergency Activities

Physical access control to a data facility/room or tape/media library poses some special problems during and after any type of emergency. The fact than an emergency occurs does not mean that access control to the GSS or MA facility or library can be ignored until the situation is corrected or has been restored to operation. Steps must be taken to ensure that only authorized persons may exit and re-enter the facility or library after an exercise, test, drill, or actual emergency.

302.4.7 Fire Safety

In most cases, DA employees are not responsible for the installation, maintenance, and inspection of fire suppression equipment or hazards. For the continued operation of the facility or library, the following should be done:

1. Conduct inspections and testing of installed fire suppression and prevention devices at the required intervals by those responsible for their inspection.
2. Conduct periodic internal inspections to find any fire ignition sources, such as potential failure of electronic devices or wiring, and improperly stored materials, especially inflammables.

3. Post appropriate evacuation instructions and assure that trained area fire marshals have been appointed and are conversant with current emergency procedures.
4. Lock fire doors to prevent entry and unauthorized use as a convenient ways to move around the facility.

302.5 INFRASTRUCTURE SUPPORT

302.5.1 Heating and Air Conditioning

The malfunction of heating, ventilation, and air conditioning (HVAC) can cause a loss of DA's IT operating capability. The following issues should be addressed:

1. A working relationship with appropriate DA and USDA organizations and personnel responsible for liaison with the GSA and its building manager to ensure that appropriate HVAC maintenance is performed.
2. Backup air-cooling system for the equipment supporting the GSS or MA facility.
3. Inspections and testing of installed HVAC equipment conducted at the required intervals by those responsible for their inspection.
4. Periodic internal inspections to find any potential obstructions to the proper flow of air through the ducts in the IT equipment area.

302.5.2 Electric power

To ensure that the GSSs or MAs has sufficient power for continuous operation, the following issues should be addressed:

1. A working relationship with appropriate DA and USDA organizations and personnel responsible for liaison with the GSA and its building manager to ensure that appropriate maintenance is performed on power management equipment in the building and the area supporting the GSSs or MAs.
2. Need for a back-up power generator with an automatic start-up capability in the event of a power failure for the equipment supporting the GSSs or MAs facility.
3. Equipment needing uninterruptible power sources (UPS) for emergency support of GSSs and MAs.

302.5.3 Telecommunications

Though the bulk of the protective measures against such entry are electronics, protecting the physical assets of the communications systems within the building housing DA's GSSs or MAs can help protect against unauthorized entry. The following issues should be considered:

1. Securing locations where communications connections are made (wire closets) within the facility housing the GSSs or MAs.

2. Assuring that all persons accessing wire closets are legitimate employees of the communications carrier or GSA or approved by the Building Manager and have met the access requirements of paragraph 302.4, above.
3. Restricting access to any wire closet outside of the facility housing the GSS or MA to authorized personnel only.
4. Ensuring that PEDs, wireless or remote, access devices, including laptop and desktop computers, and their peripherals use only approved dial-up and broadband access to the GSS and its MAs. As part of the remote access documentation, the DA will maintain records detailing individual remote connections to include connection type and vendor.

302.5.4 Other

Other utilities can malfunction and cause operating problems for a GSS and/or MA. To ensure that this type of situation does not occur, the following issues should be addressed:

1. Impact of threats to power distribution, heating plants, and water and sewerage facilities and other utilities.
2. Plumbing lines in the vicinity of the data facility/room and tape/media storage area.

302.6 WIRELESS, REMOTE, OR PORTABLE SYSTEMS

Mobile or portable data equipment that will communicate with, or contain information found in, a DA GSS or MA poses special physical and environmental security problems. These kinds of equipment include, but are not limited to, wireless, remote, portable or similar devices, such as, laptop and desktop computers, PDAs or PEDs, e-mail capable cell phones, portable storage drives and disks, and other similar devices. Because of their portability or use for telecommuting, these devices must be handled in a manner that reduces the threat of theft or the surreptitious addition of harmful programs or the surreptitious access to or the removal of information. Procedures must be developed to:

1. Allow the use of wireless, remote, portable, or similar devices, such as, laptop and home computers, PDAs or PEDs, e-mail capable cell phones, portable storage drives and disks, and other similar devices access to the GSS and MAs only after receiving written authorization to access the DA GSS and its MAs from the DA CIO.
2. Maintain an Inventory of all wireless, remote, or portable and other similar devices, their peripherals, and software by serial number under the control of each DA Staff Office or that are providing sensitive information to or taking sensitive information from, a GSS or MA.
3. Maintain strict accountability by serial number of all wireless, remote, or portable and other similar devices and peripherals issued to DA and DA contractor personnel by requiring a signature upon issuance that is maintained with other accountable records.
4. Provide written authorization from the DA CIO to each person provided DA wireless, remote, portable, or other similar devices or peripherals before allowing access to a GSS or MA.

5. Prior to the issuance of a device or peripheral, the recipient must have completed the required form requesting their issuance and use. Additionally, the recipient must sign an acknowledgement of understanding the “DA Personal Use Policy”, the original copy of which will be maintained with the accountability records for the device issued.
6. Ensure that all PEDs, and wireless and remote access devices, including laptop and desktop computers, and their peripherals, are appropriately marked or tagged and appropriately labeled with contact information to allow the tracking of the device or finding it if it is lost.
7. Ensure that when not in use, PEDs, and wireless and remote access devices, including laptop and desktop computers, and their peripherals must be stored in a secure location.
8. Ensure that when the user travels the device(s) must be hand carried and under control of the user at all times. When not in use the device must(s) must be powered off.
9. Provide appropriately documented authorization for an employee to download Sensitive but Unclassified (SBU) information to wireless and remote access devices, including laptop and desktop computers, and their peripherals for work away from the office. This documentation may be included in the request for use of these devices.
10. Maintain a log of persons allowed access to the GSS or MA using wireless, remote, portable devices that shows the person’s full name, organization, contact information, date of issue of the equipment, and the date of its return.
11. Require unique user ID and password for any person allowed to use wireless, remote, portable, or other similar devices to access and upload sensitive information to the GSS or MA or download information from it to a wireless, remote, portable or other similar device. The protocols used for establishing and changing these passwords will be in accordance with USDA password protocol guidance.
12. Ensure passwords and IDs are changed every ninety (90) days and appropriately reflected in the log.
13. Software that will identify that sensitive information has been downloaded from a GSS or MA workstation to a device or drive other than the workstation’s hard drive.
14. Prior to each turn-in, the PEDs, Laptop or desktop computer, and peripherals must be checked to ensure user profiles, user data files, and any “user unique” software applications have been removed and that software applications authorized by DA are installed on the item(s). The same check is to be made upon issuance of the item(s).
15. Disciplinary actions for unauthorized persons attempting to access, upload, or download information to or from a GSS or MA.

302.6.1 Certify and Registration of Remote Computers

Virus attacks on networks have emphasized the importance of configuration management in ensuring the security of the network. In order to ensure and provide vulnerability and virus protection to DA users all remote users with laptops or PCs must have the machines certified and registered by the DA CIO before the computers are allowed access to DA network. Remote computers are machines used outside of the USDA facilities. Users of DA network may be USDA employees or contractors working on USDA projects. DA remote computers must maintain a standard configuration of applications and utilities. The DA Standard Desktop Configuration is presented in Appendix E. The information captured during the certification and registration process is also presented in Appendix E

DA will conduct the certification and registration quarterly and by staff offices. The process will require users to bring in there computers to DA IRD, DA IRD Help Desk will review the configuration, update the configuration as needed, document the configuration and return the computer at the end of the working day. Detailed procedures to certify and register remote users are also contained in Appendix E.

302.7 MANAGEMENT CONTROLS.

302.7.1 Review of Procedures

The physical and environmental security procedures for each GSS and MA location must be reviewed and, if needed, updated annually. They must also support or provide audit trail information associated with any breach of security related to a GSS or MA.

To effectively control the access to the GSS or MA facility/room or library, certain management and administrative activities must occur to enhance the access controls. The following issues should be addressed:

1. Audit trails that accurately reflect the access to and exit from the facility/room or library.
2. Prompt investigations of any security violations, including suspicious physical access activity, and remedial actions taken.
3. Pre-planned appointments and identification checks to authenticate visitors, contractors, and maintenance personnel before allowing their access.

302.7.2 Security Awareness Training

To ensure that the above instructions are understood, they are to be included in the security awareness and training programs that are provided to DA and DA contractor employees, and employees of other organizations that can visit the facilities/rooms containing a DA GSS or MA or access its sensitive information.

303 PRODUCTION, INPUT/OUTPUT CONTROLS

303.1 PURPOSE

This procedural guide provides managers with the information needed to establish IT security controls that ensure the adequate security of input, production, and output processes, documents, and media within their organization. It aids them to establish their organization's procedures to receive, store, handle, and destroy information and its electronic data or printed media. The procedures also aid in protecting DA data from intentional or accidental viewing, use, or manipulation by persons not authorized to do so. The procedures must also cover the use of DA issued wireless, remote, portable, or other similar devices.

303.2 SCOPE

These guidelines apply to all GSSs and MAs in the operation and maintenance phases of the Systems Development Life Cycle.

303.3 ROLES AND RESPONSIBILITIES

303.3.1 CIO

The CIO is responsible for assuring staff offices governing the production, input, and output of data used by their employees and contractors establish the appropriate procedures.

303.3.3 DA Staff Office Directors

DA Staff Office Directors are responsible for establishing appropriate controls governing the production, input, and output of the data used by their employees and contract employees.

303.4 PROCEDURES

The procedural information below provides guidance to ensure that all DA executives, managers, and employees maintain appropriate and adequate control over all data when accessing, entering, manipulating, or extracting data from any IT system for any purpose. The procedures in the following sections must be established as a minimum within each Office, to ensure minimum compliance with current USDA and federal information technology security standards. The procedures also apply to, wireless and remote access devices, including laptop and desktop computers, and their peripherals, and must be designed to:

1. Prevent the theft of electronic data and printed media;
2. Prevent the unauthorized reading, copying, or altering of electronic data or printed input or output media;
3. Prevent unauthorized remote access.
4. Ensure that SBU information is transmitted or stored in an encrypted state. The Departments Virtual Private Network (VPN) or equivalent product is to be used for SBU transmissions from all authorized remote locations.

5. Ensure that only authorized persons pick up, deliver, and/or receive electronic data, printed input or output media, and wireless and remote access devices, including laptop and desktop computers, and their peripherals;
6. Ensure the proper storage, labeling, transfer, and transportation of electronic data or printed input or output media;
7. Establish destruction requirements for electronic data, printed input or output media, and USDA wireless and remote access devices, including laptop and desktop computers, and their peripherals to prevent unauthorized access to the information contained on the them; and
8. Establish appropriate and complete audit trails related to the access to electronic data or printed input, storage, or output media, and wireless and remote access devices, including laptop and desktop computers, and their peripherals and the facilities that house them.

303.4.1 User Support

Procedures must be established to ensure that DA authorized IT users can obtain timely and appropriate help desk assistance with security problems related to their use of a DA IT system or application. These procedures must address actions to be taken in response to security incidents, and must be accessible to each user and to the help desk personnel.

303.4.2 Access and Authorization

Staff Office production, input, and output procedures must define the persons or job positions that are authorized to access printed, handwritten, and electronic input and output information and media. The procedures may be designed to allow the access of one group of persons to a specific input and output activity while excluding the access of other groups having access to other specific areas. The information related to the authorization must be sufficiently clear to ensure that the requirements in paragraph 303.1, above, are met. Procedures must address:

1. The information security requirements established in the *DA IT Security Policy Instruction*.
2. Password controls and their use to ensure their security and prevention of their misuse. Password control guidance to users must be explicit.
3. The need to ensure that the screensaver used on a computer is password protected and timed to begin operation after no more than ten (10) minutes of the computer's non-use. The screensaver must require the use of the password to access the monitor for work purposes. All wireless and remote access devices, including laptop and desktop computers must have the screensaver's password function enabled.
4. The requirement that each user must log off the computer but turned on at the end of each workday.

5. Sufficient information related to the storage, labeling, and destruction of input and output media as to reduce the potential theft or misuse of information and media when the user has it under his/her control.

303.4.3 Labeling Printed and Electronic Media

To ensure that DA is appropriately and adequately protected, office procedures must require that printed, handwritten, and electronic input and output information and media are appropriately labeled. Labels must include the title of the data, indicate its sensitivity, and state any special handling instructions as required by current USDA and DA guidance with regard to classified, Privacy Act, internally sensitive, and proprietary information.

303.4.4 Storage and Destruction

Storage and destruction of information and storage media must be addressed in accordance with current USDA and DA IT requirements. The procedures must also include those applicable to DA issued wireless, remote, portable, or other similar devices. The procedures should consider:

1. Where printed, handwritten, electronic media, wireless and remote access devices, including laptop and desktop computers, and their peripherals are to be stored, the procedures must ensure that storage methods meet USDA physical security requirements.
2. The specific storage locations, (vaults, file cabinets, libraries), that provide the security needed be consistent with the level of protection required for its sensitivity rating.
3. The methods and accountability procedures to be used to sanitize printed, electronic input, output media or and wireless and remote access devices, including laptop and desktop computers, and their peripherals prior to their reuse be based on the sensitivity of the information found on the media.
4. How damaged media is to be stored until it can be thoroughly destroyed. Since certain types of printed and electronic input, output information and their media, and wireless and remote access devices, including laptop and desktop computers, and their peripherals pose special sanitizing problems when damaged, the procedures must specify how they are to be destroyed.
5. The requirement that offices have a crosscut shredder available for destroying damaged and undamaged printed media information.

303.4.5 Audit Trails

Audit trails must be established for the activities governing the input and output of printed, handwritten, electronic information and media that are sufficient to reconstruct a security event. A reconstruction is needed to determine the way security was breached and/or information was lost, so steps may be taken to prevent such a breach or loss in the future.

Access to this audit trail is to be limited to authorized personnel and is to be protected from unauthorized access or modification that may negate its forensic value. All audit information must be retained and reviewed in accordance with USDA OCIO policy.

303.4.6 Record Contents

The audit trail record should contain:

1. The IT system's name, the user's name or user ID, the date(s) and time(s) for each physical or electronic entry into and exit from the sensitive system or the facility housing a sensitive system.
2. A record of the activities performed when sensitive data, information, or a facility/room housing the system is accessed.
3. If electronic recording procedures are used to monitor access, any activities that could alter the integrity of the information, allow future alteration of the information, or allow the bypassing of system controls.
4. Information that supports an after-the-fact investigation to determine how, when, and why an event caused a major interruption of, or ended, normal operation or caused a loss of data.

303.5 MANAGEMENT CONTROLS

303.5.1 Audit Trail

Procedures that implement the activities below will assist managers in fulfilling their security audit trail responsibilities. Managers, in accordance with DA IT security guidance, are to establish procedures that:

1. Strictly control the access to online audit logs;
2. Require the review of audit trails on a monthly basis;
3. Establish the controls for access to off-line audit logs in accordance with paragraph 303.4, above, for sensitive information;
4. Support the audit procedures outlined in Section 403, Audit Trails.

303.5.1 Training

Managers, both federal and contractor, must provide appropriate training to employees to carry out the procedures described above. This training must include the specialized training required for persons designated to maintain and protect the forensic viability of audit trails and logs. Additionally, Security Awareness Training must be provided to both federal and contract personnel to assure they are aware of the security procedures and the penalties for violating them.

304 CONTINGENCY PLANNING

304.1 PURPOSE

IT Contingency-Disaster Recovery Plans (C-DRP) are developed for each GSS and MA to assure timely restoration and resumption of operations should the systems be destroyed or fail to operate.

304.2 SCOPE

A C-DRP must address circumstances within the control of DA as well as those outside of DA's control. Priorities must be assigned to GSSs and MAs for protection and restoration. The *IT Contingency and Disaster Recovery Planning, CS-028* provides guidance in establishing contingency/disaster recovery plans.

304.3 ROLES AND RESPONSIBILITIES

304.3.1 CIO

The CIO is responsible for ensuring that USDA contingency planning policy is uniformly applied across DA organizations and for coordinating DA disaster recovery planning efforts. The CIO will review and approve each DA organization's system-specific C-DRPs.

304.3.2 DA Staff Office Directors

DA Staff Office Directors are responsible for developing C-DRPs for each GSS and MA under their control. They are also responsible for assuring that C-DRPs are tested and that deficiencies found during testing are corrected.

304.4 PROCEDURES

Every GSS and MA must have an IT Contingency-Disaster Recovery Plan (C-DRP). The C-DRP must address each contingency scenario from the temporary loss of electricity to a server up and running, permanent loss of the processing facility. C-DRPs for MAs must be coordinated with the Contingency Plans for the supporting GSS to ensure that they are complementary. OCIO guidance establishes the methods and procedures to be used by DA when developing contingency/disaster recovery plans.

304.4.1 Purpose

The C-DRP is used to plan for, respond to, recover from, and restore DA's IT business operations in the event of a natural or technological disaster. These plans must ensure the timely restoration and resumption of DA IT systems and applications if they are destroyed or fail to operate. "Timely" restoration is defined for each system in accordance with the availability factor in the system sensitivity matrix.

304.4.2 Considerations

The following must be considered when developing a C-DRP.

1. All C-DRPs prepared for DA GSSs and MAs must be based on the OCIO template provided.

2. Planning must consider requirements to support the C-DRPs of other USDA agencies. DA IT managers must coordinate their contingency-disaster recovery planning with USDA agencies, as appropriate.

3. The C-DRP developed for each MA must address the complete range of situations that may impair processing, from temporary loss of a single server supporting only that MA to complete long-term loss of all processing support as a result of a disaster such as a fire or explosion in the data center.

4. C-DRPs must be tested annually and the test results must be evaluated. If this evaluation indicates plan deficiencies, the deficiencies must be corrected in a timely manner as determined by the Staff Office Director in consultation with the CIO.

304.5 MANAGEMENT CONTROLS

DA managers will ensure that C-DRP activities are carried out as described in the *DA Contingency Planning/Disaster Recovery Planning Guide* (under development).

305 HARDWARE AND SOFTWARE SYSTEM MAINTENANCE

305.1 PURPOSE

These procedural guidelines will assist any DA organization in establishing effective hardware and software maintenance management procedures. They will ensure that installation, change, and updating procedures adequately reduce the risk of damage or destruction of GSSs and MAs when maintenance is performed. Effective procedures will help ensure that installation, change, and updating of hardware and software are adequately addressed to reduce the risk of damage to or destruction of GSSs and MAs when maintenance is performed.

305.2 SCOPE

These hardware and software management and maintenance guidelines apply to all DA organizations and are to be applied to all DA GSSs and MAs. This guidance must be used when establishing hardware and software maintenance procedures.

305.3 ROLES AND RESPONSIBILITIES

305.3.1 CIO

The CIO is responsible for ensuring that hardware and software maintenance policies, procedures, and practices for GSSs and MAs are established and followed. The CIO must approve procedures and ensure that adequate resources are planned for hardware and software maintenance performed on a GSS or MA.

305.3.2 DA ISSPM

The DA ISSPM should ensure the development of guidance related to the hardware, peripherals, firmware, and software that are appropriate to DA systems and oversee its implementation, and restricting their installation only to DA authorized personnel. This includes the hardware, peripherals, firmware, and software associated with remote access functions**.**

305.3.3 DA Staff Office Directors

The DA Staff Office Directors must develop appropriate maintenance guidelines and procedures to protect any GSS and MA under their control, in accordance with *DA Information Technology Security Policy Instruction* and the appropriate SSP.

305.4 PROCEDURES

305.4.1 General

The following must be included in the hardware and maintenance procedures for all operating systems.

1. Only DA authorized and up-to-date hardware, peripherals, firmware, and software, including that used for remote access, are to be installed and used to access the DA GSS and MAs.
2. All operating and remote access systems and peripherals should be configured to prevent the circumvention of the software and application security controls. If it is determined that the configuration/change cannot adequately achieve this goal, measures must be taken to identify any successful or unsuccessful attempt to circumvent those controls and, if possible, identify the perpetrator.
3. All system files and directories, including those used for remote access, must be marked as “Read Only.”
4. Regularly scheduled hardware and software maintenance reviews, including those made of items used for remote access, must be conducted on each GSS and MA to ensure that appropriate updates have been made or are scheduled. Hardware and software maintenance reviews are conducted to assess the impact when a change is

made to (1) a GSS or MA; (2) the facility housing it; or (3) other environmental conditions that may affect security and maintenance requirements.

5. Systems technicians must have up-to-date reports related to the maintenance, security, and functionality for systems including DA issued and privately held wireless and remote access devices, including laptop and desktop computers and their peripherals.
6. All hardware and software maintenance activity should be fully documented and include the names of the persons performing the maintenance, as described in Section 307.
7. A Configuration/Change Management process should be in place to control the installation of products, versions of software or firmware, and other changes to a GSS or MA as described in Section 307.
8. A list of companies or organizations authorized to perform hardware and software maintenance on DA systems, GSSs, and MAs, including those applicable to PEDs, wireless and remote access devices and their peripherals, should be developed and maintained.

305.4.2 Specific Hardware and Software Procedures

The following specific actions must be included in the hardware and software procedures for all operating systems.

1. A roster of the persons authorized to perform hardware and software maintenance for systems, GSSs, or MAs must be maintained.
2. Appropriate steps to ensure that maintenance personnel cannot access system libraries unless authorized by the SM must be taken. Such access to libraries is to be strictly monitored.
3. Systems maintenance personnel must be under continuous escort by a DA IT employee with the ability to determine the appropriateness of the maintenance person's actions and to prevent unauthorized access to the system, unless authorized by the CIO.
4. Hardware devices, including wireless and remote access devices (including laptop and desktop computers) and their peripherals, must be sanitized before they are removed from the site for maintenance or destruction.
5. When hardware devices, including wireless and remote access devices (including laptop and desktop computers) and their peripherals, are removed from the location for maintenance or destruction, an inventory of the device(s) must be prepared. The inventory must show the make and model of the device, its serial number, the person who took control of the device, and the company for which that person works.
6. The distribution and implementation of new or revised software must be documented and reviewed to ensure it has been effectively done and the configuration management process is followed.

7. When system maintenance is performed remotely, including that provided for wireless and remote access devices (including laptop and desktop computers) and their peripherals, remote access must be de-activated when maintenance is complete.

305.4.3 Testing and Approving Hardware and Software Use

Hardware, including wireless and remote devices (including laptop and desktop computers), software, firmware, and/or peripheral device changes or installation must be properly authorized, tested, and approved for their system, GSS, or MA. The authorization, testing, and approval process must ensure that:

1. The installation or change of hardware or software, including wireless and remote access devices (including laptop and desktop computers) and their peripherals, must be in accordance with USDA and DA change management process requirements and must include the submission of required Certification and Accreditation packages.
2. Hardware and software changes are tested, approved, and documented prior to their being placed into production. Actual or "live" data currently residing on the system, GSS, or MA must not be used for the testing. Information from a stored backup tape may be used, provided the data is over three (3) months old and is not on the most recent set of backup tapes. If it is not feasible to use the backup tape, then "dummy" or made up data must be used.
3. The development of additional non-IT security measures to mitigate the impact of potential threats that may occur during the testing process.
4. An appropriate level of risk for the testing of the system, GSS, or MA is determined. The recommended level of risk may be based on a cost benefit analysis of the potential impact of a threat and the steps needed to protect against that threat.
5. Software programs are appropriately labeled and documented after each change. These labels must include version, date of change, implementation date, and other relevant information related to the change.

305.4.4 Vulnerability Control and Patch Management

The actions listed below will provide a minimum level of vulnerability control.

1. The most restrictive security settings must be used as default settings during testing and the initial installation phase when software and hardware are being changed.
2. Security settings may be returned to their operational mode after the initial installation of the tested change is completed. However, at no time are the security settings for the hardware or software, including passwords, to be the manufacturer's default settings.
3. GSSs and MAs must be reviewed on a regular schedule to identify and, when possible, eliminate unnecessary services that can lead to a breach of security or provide unauthorized access. (For example, FTP or HTTP protocols, mainframe supervisor calls, etc.)

4. GSSs and MAs must be reviewed on a regular schedule to determine vulnerabilities and to ensure that software patches are promptly installed to reduce those vulnerabilities.

305.4.5 Patch Link Tool

DA has implemented a Patch Link tool and service to support the

GSS network environment. The network engineers maintain the DA Patch Update Checklist in the computer room. The procedures and checklist are presented in Appendix D. The procedures include:

1. Review new patches provided from the Patch Link Service to assess if needed in DA's computing environment. DA engineers must ensure that the patches are tested and certified by the Patch Link service prior to deployment.
2. The CIO must grant permission before any patches can be scheduled or deployed to the GSS for pushing to the computers on the DA network.
3. The new patch must be added to the computer patch baseline for new PC connecting to the network so that all patches will be deployed to the new PC.
4. Approved wireless and remote access devices (including laptop and desktop computers) and their peripherals, must contain only software applications approved and licensed in accordance with USDA policy.
5. Frequent checks are to be made for licenses, up-to-date patches, and approved software for authorized DA issued and privately owned wireless and remote access devices (including laptop and desktop computers) and their peripherals.

305.5 MANAGEMENT CONTROLS

305.5.1 General

To effectively manage hardware and software installation and maintenance activities, managerial controls that complement operational procedures must be implemented. The use of these controls will ensure that all hardware and software maintenance activities are carried out in a manner that protects the integrity of each GSS and MA and the data they house. These management controls are:

1. A risk analysis must be conducted to determine the effect that any changes to a GSS or MA caused by hardware and software maintenance will have on its security controls. The analysis must also include the impact upon the training needed to implement and manage any changes in the security controls affected by hardware or software changes.
2. A Configuration/change Management (CM) System must be used to manage the changes to a GSS or MA caused by hardware and software maintenance activities. This CM system must meet USDA OCIO and DA CM requirements.

3. Required USDA OCIO or DA software implementation distribution orders that clearly state the effective date on which all appropriate locations are to implement the change(s) in the order must be followed.
4. Only software licensed to DA may be used when changing a system, GSS, or MA under its control.
5. Up-to-date procedures for using, and monitoring the use of, system utilities must be established and maintained.
6. An emergency process that satisfies USDA OCIO and DA requirements for hardware and software maintenance must be developed, approved, and maintained. Each implementation of that emergency process must be justified and approved within 15 days after the emergency process is used.
7. Security related documents must be changed appropriately as hardware and software maintenance is performed on GSS or MA components, e.g., contingency or disaster recovery plans, etc.

305.3.1 Hardware and Software Maintenance Training

Offices must provide appropriate training to all employees as follows:

1. Managers must be provided with the specialized training required for persons responsible for developing and overseeing the compliance with and use of the DA hardware and software maintenance procedures as part of their duties.
2. ISSOs must undergo hardware and software maintenance procedure training. Appropriate levels of training will, at a minimum, familiarize them with the hardware and software maintenance procedures and, if software programs are used to record this maintenance, the use of the software programs.
3. Each System Manager (SM) must receive training on the conduct of hardware and software maintenance related to DA IT systems in general and specifically to the GSS and MA support for which they are responsible. Appropriate levels of training will, at a minimum, familiarize them with USDA OCIO and DA hardware and software maintenance procedures and, if software programs are used to record this maintenance, the use of the software programs.

306 DATA INTEGRITY

306.1 PURPOSE

Data integrity includes the controls used to protect DA data from accidental or malicious alteration. These controls provide the user with the assurance that the data meets expectations about quality and integrity. Validation controls are comprised of the various tests and evaluations used to determine compliance with security specifications and requirements.

306.2 SCOPE

Data integrity requirements apply to all GSSs and MAs.

306.3 ROLES AND RESPONSIBILITIES

306.3.1 CIO

The CIO is responsible for oversight of the data integrity/validation controls utilized on all GSSs and MAs. The CIO will establish and monitor validation-testing programs.

306.3.2 DA Staff Office Directors

DA Staff Office Directors are responsible for assuring that data integrity/validation controls are developed, tested, documented, and implemented for the GSSs and MAs under their control.

306.4 PROCEDURES

306.4.1 Virus Detection and Elimination

1. Virus detection software installed on DA systems must be routinely updated.
2. All DA virus detection systems are to automatically scan any new data files loaded into the system from any source.
3. All hardware, including wireless and remote devices (including laptop and desktop computers), and their peripherals, must have approved virus protection software installed in then, have an up-to-date version, and have an updated signature file.

306.4.2 Integrity and Validation Controls

The methodologies listed below will assist in the control of the integrity and validity of the data in and operation of the GSS and its MAs.

1. Reconciliation routines should be used on all DA IT systems and applications. The software, among other actions, must provide checksums, hash totals, and record counts.
2. Appropriate software and hardware should be used to detect and record intrusions from external and internal DA sources.
3. DA IT system managers will analyze real time performance logs to determine availability problems, including attacks. Whenever inappropriate or unusual activity is found, they will immediately initiate appropriate investigative action and report the matter to DA IT security officials.

306.4.3 Wireless and Remote Access Device Access

The use of wireless and remote access devices, including laptop and desktop computers, and their peripherals pose special security issues that can severely impact the integrity of the GSS, its MAs, and their applications and data. The uses of appropriate encryption/decryption algorithms in conjunction with passwords and other security features can reduce potential adverse impacts. To reduce possible adverse impacts, the following must be done.

1. Encryption used by the DA GSS and its MA, including that used by remote access devices, must conform to USDA and NIST approved algorithms used for data encryption/decryption.
2. Users of Wireless and remote access devices, including laptop and desktop computers are prohibited from changing or disabling the encryption/decryption settings on the devices.
3. The use of encryption/decryption mechanisms must be configured to ensure that data files are encrypted on a per record basis. This will ensure that, if a device is lost or stolen, an unauthorized person would only have access to the current working document.
4. Any SBU information received from, sent to, or stored on a PED, wireless or remote access device, including laptop and desktop computers, and their peripherals must be encrypted and decrypted in accordance with USDA and DA policy using USDA and NIST standards.
5. The USDA Virtual Private Network (VPN) or an equivalent product is to be used for the transmission of SBU information using a PED, wireless or remote access device, including laptop and desktop computers, and their peripherals. When the VPN or equivalent is used, split tunneling profiles on the devices are to be disabled.

306.4.4 Protective Scans

Scanning networks and systems is done for three reasons. The first is to determine if a person outside the network or system is attempting to find an entry point to use to penetrate the system or subsystem. Secondly, to determine if someone authorized access to part of the network or system is attempting to penetrate a system or subsystem they are not authorized to access> the third is to determine if someone within the system is attempting to use the system in violation of USDA and DA policy and procedures. Effective scanning also facilitates the use of software designed to trace an external scan and internal attempt to penetrate a system or subsystem back to its point of origin. A protective scanning program requires that each DA System Manager:

1. Establishes a continuously operating external and internal scanning program designed to detect the three purposes listed above.
2. Has the capability of detecting and tracking scans on system entry points to the origin of the scan.

3 Monitors activity within the their system and its associated network infrastructure to determine if persons are attempting to gain access to information they are not authorized to access and determine where the attempt is originated. E.g., a DA employee attempting to gain information from a personnel database that they are not authorized to access.

4. Monitors activity within the system to determine if system users are exploiting system assets for unauthorized purposes. E.g., determining if a DA employee is accessing unauthorized or prohibited web sites, excessively using e-mail or instant messaging, etc.

306.4.5 Penetration Tests.

Penetration testing allows the CIO, system administrators and system managers to protect the availability, integrity, and confidentiality of information in the DA GSS and its MAs. A penetration testing program meets the following requirements.

1. Each DA System Manager will establish an external and internal penetration-testing program designed to validate the installed intrusion detection system's operation and the effectiveness of the IT reporting and response mechanisms.
2. The penetration-testing program will test each potential entry point on the system that could allow entry by persons both inside and outside of the system.
3. The penetration-testing program will be a continuous program that tests each MA and GSS and its entry points.

306.4.6 Integrity and Validation Control Records

Records generated from activities designed to ensure validate and protect the integrity of the DA GSS and its MAs must be handled and protected in the same manner as Audit Trail records, as discussed on Paragraph 403, Audit Trails, below.

306.5 MANAGEMENT CONTROLS

Data integrity procedures will be designed to ensure compliance with the DA password policies and procedures.

307 DOCUMENTATION

307.1 PURPOSE

The documentation of hardware, software, policies, standards, procedures, and approvals required by DA provide the basis for protecting the integrity, availability, and confidentiality of DA IT systems

307.2 SCOPE

A list of documentation must be developed and maintained for each GSS and MA for its Systems Development Life Cycle.

307.3 ROLES AND RESPONSIBILITIES

307.3.1 CIO

The CIO is responsible for providing guidance and reviewing appropriate system security documentation.

306.3.2 DA Staff Office Directors

DA Staff Office Directors are responsible for ensuring that system security documentation is developed and maintained for all GSSs and MAs under their control.

307.4 PROCEDURES

Documentation explains how software/hardware is to be used and formalizes security and operational procedures specific to each system. Descriptions of hardware and software, policies, standards, procedures, and approvals related to automated information system security in each MA and GSS, backup and contingency activities, and descriptions of user and operator procedures should all be included. The following documentation should be produced, available, and current for all GSSs and MAs, in accordance with the requirements of the USDA OCIO:

1. System Security Plan;
2. Contingency Plan;
3. Risk Assessment;
4. Rules of Behavior;
5. Certification and Accreditation documents and statements that authorize a system to operate;
6. Standard operating procedures for users, system administrators, ISSOs, DA Staff Office Directors and other managers in accordance with this document;
7. Configuration/change Management Plan; and
8. Functional Description (Functional Requirements Document) Document.

307.5 MANAGEMENT CONTROLS

Documentation for MAs should be coordinated with the supporting GSS and/or network manager(s) to ensure that adequate applications and installation documentation are maintained to provide continuity of operations.

308 SECURITY AWARENESS AND TRAINING

308.1 PURPOSE

Security awareness and training provide a level of understanding of the need for security measures, DA's expectations for users accessing their GSSs and MAs, and the liabilities for both DA and individuals in not adhering to security measures.

308.2 SCOPE

Security awareness and training is mandatory for all employees who are involved with the management, use, or operation of a federal computer system within or under the supervision of a federal agency. Security awareness and training must be provided before initial access to such systems and on a periodic refresher basis.

308.3 ROLES AND RESPONSIBILITIES

308.3.1 CIO

The CIO is responsible for ensuring that:

1. An adequate IT security awareness and training program, including that related to the use of wireless and remote access devices, including laptop and desktop computers, and their peripherals is being provided to DA employees and contractors;
2. Lists of individuals who received training, and the types of training they received are maintained for two (2) years;
3. The IT security awareness and training program is developed and maintained in accordance with the USDA OCIO guidance.

308.3.2 DA Staff Office Directors

DA Staff Office Directors have overall management responsibility for the development of security awareness programs for the particular GSS or MA systems under their control. They are responsible for:

1. Assuring that all of their employees and contractors have attended security and awareness training sessions at the recommended times;
2. Verifying that employees and contractors receive training that is adequate and appropriate to the GSSs or MAs they utilize;
3. Maintaining a list of individuals attending training, and the type and frequency of this training; and
4. Assuring that warning banners are presented in a timely fashion and contain the appropriate language.

308.4. PROCEDURES

308.4.1 Coverage

SSPs for all GSSs and MAs must contain security awareness information. This should include type and frequency of training. Security awareness training must encompass rules of behavior for specific GSSs and MAs, and for wireless and remote access devices, including laptop and desktop computers, and their peripherals, and incident reporting procedures. This training must be provided prior to being allowed access to the GSS or MA. The training should be given as part of new employee orientation. Contractor training should be given as part of project orientation. Refresher training should be conducted annually.

308.4.2 Wireless, Remote, or Portable Device Training

308.4.2.1 General

In the event that DA issues wireless, remote, or portable devices, such as, laptop and home computers, PDAs or PEDs, e-mail capable cell phones, portable storage drives and disks, and other similar devices to allow remote access to the GSS and its MAs, the users of the devices must be provided additional security awareness training. This training must include; but not be limited to, the use of and the security issues related the use of portable, wireless, and remote devices, including laptop and desktop computers, and their peripherals, or other similar devices, liability for loss of a device, and any other security issues related to the use and safeguarding of the information the device contains.

308.4.2.2 Specific

Users must be aware of the DA "Personal Use Policy" related to DA wireless, remote access, or portable devices, the need to update virus detection programs, that the USDA retains the right to delete or purge data on wireless and remote access devices, including laptop and desktop computers, and their peripherals, even when remote access is authorized for a privately owned device. These users must understand the procedures used for secure remote access arrangements, the storage of encrypted SBU data the authentication procedures used for remote access, and that they cannot reconfigure the system BIOS. Due to the nature of remote access devices, each user must be fully aware of the procedures to follow should they lose a DA issued or private devices issued for use to access the GSS and/or its MAs.

308.4.2.3 Acknowledgement

Users of wireless and remote devices, including laptop and desktop computers, and their peripherals must provide a signed acknowledgement of training on their use and their security requirements, including their understanding of the DA "Personal Use Policy," prior to the submission of a request for the issuance of a USDA issued device or for the authorized use of privately owned devices and peripherals. A copy of this acknowledgement is to be retained with the authorization for the used of these devices.

308.4.3 Role-based Training

Training should be role-based. All employees should receive training on password usage, rules of behavior, incident reporting, and other security procedures. Applications developers should receive additional training in areas such as guidelines for applications development control over test passwords, and separation of duties. System administrators should receive additional training in the use of audits, user account management, access permissions, and other relevant areas.

308.4.4 Intranet Library

Final versions of all DA ITS documents must be maintained on a DA ITS Intranet site. The program offices will provide the CIO with the final version of all ITS documents for inclusion on this site.

308.4.5 Employee Warning Banner

The following is related to the use of banners for DA GSS and MAs:

1. All DA IT systems require a banner that warns employees that accessing the system constitutes consent to monitoring for law enforcement and other purposes and must be the first screen seen before allowing a logon to the GSS or its MAs. The banner must also contain a warning to unauthorized users that their misuse of the system may subject them to criminal prosecution. This section addresses the preparation and presentation of employee warning banners. The banners must be highly visible and must be presented in a timely fashion. Each SSP indicates what the banners are to contain and when they are to be presented to the user. Each user, whether directly or remotely connected to the GSS or its MAs, must acknowledge their understanding of the banner prior to logging-on.

2. Banners are presented when the user first attempts to log on to the system from either a remote location or using a direct connection. As an option, a second presentation may occur when a successful log on has been made.

3. A copy of the banner as presented should be included in both system documentation and training materials.

4. Public Law 99-474 requires that a warning message be displayed; notifying unauthorized users that they have accessed a U.S. Government computer system and unauthorized use can be punished by fines or imprisonment. Some of the systems now in use are intended for unrestricted use by the general public (e.g., Internet-based systems used for widespread public information dissemination); a situation not prevalent when Public Law 99-474 was enacted. Due to their adverse impact on the intended user population, highly restrictive warning banners may not be appropriate. The choice of which screen warning banner to implement is up to the system owner and should be

based on system-specific technology limitations, data sensitivity, or other unique system requirements.

5. SSPs must describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the Department of Justice (DOJ), Computer Crime and Intellectual Properties Section, approved the warning banner. Examples of banners currently approved by DOJ are shown in Figure 308.4

6. When the system is modified, or its use or users are changed, the banner warning and method of presentation should be examined to assure that it is still appropriate.

7. Banners should be reviewed annually to assure that the warning is relevant. In addition to the banner, rules of behavior should be posted as part of the log on process for each GSS and MA.

308.4.6 Additional Awareness Materials

Posters, e-mail messages, booklets, fliers, and other reminders may be used to ensure that system users are aware of the importance of knowing and adhering to IT Security program policy.

Figure 308.4 Sample Warning Banners

Banner	Selection Rationale
WARNINGWARNING**WARNING** This is a (Agency) computer system. (Agency) computer systems are provided for the processing of Official U.S. Government information only. All data contained on (Agency) computer systems is owned by the (Agency) *may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner,* by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may give to law enforcement officials any potential evidence of crime found on (Agency) computer systems. *USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, OR CAPTURING and DISCLOSURE.* **WARNING**WARNING**WARNING**	System is for Government use only and all transmissions may be monitored.
WARNINGWARNING**WARNING** This is a United States (Agency) computer system, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action. All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Access or use of this computer system by any person whether authorized or unauthorized, constitutes consent to these terms. **WARNING**WARNING**WARNING**	System is for Government use only. Monitoring is only performed in support of system operations and when investigating potential security events.

308.5. Management Controls

308.5.1 General

Managers must assure that employees and contractors complete training and that the training is adequate. Program offices should develop procedures for establishing a training curriculum for each employee based on his/her role relative to the GSS or MA. Program offices must maintain records of training courses taken by employees and must maintain these records for two (2) years. This information will be provided to the CIO on an annual basis.

308.5.2 Training Course Reviews.

Program offices should initiate regular reviews of security training courses. Reviews should be conducted if one of the following conditions occurs:

1. An adverse finding from an internal or external security controls review,
2. An incident resulting from inadequate training, or
3. A major change to the GSS or MA system.

Absent these specific conditions, conduct reviews annually.

309 INCIDENT HANDLING, RESPONSE, AND REPORTING

309.1 Purpose

The *USDA Computer Incident Response Procedures Manual, DM-3500,* provides general guidelines and procedures for handling computer security incidents. The term *"incident"* is defined as any occurrence that has been assessed as having an adverse effect on the security or performance on any part of a DA computer system. The document describes actions to be taken when a security incident is discovered. The response is required to ensure that the incident has not affected the availability, integrity, confidentiality, or continuity of an IT system. The reporting is required to assure that vulnerability and threat information is shared with interconnected USDA and government systems, and with the central organizations that monitor security incidents.

309.2 Scope

Any and all incidents discovered on a DA application or network, including Regions, Job Corps, and Office Workforce Security, are covered by this procedure. Any network with direct connection to a DA network and all non-DA sites processing DA data must also notify DA immediately upon discovery of security incidents.

309.3 ROLES AND RESPONSIBILITIES

309.3.1 Incident Response Team

The Incident Response Team (IRT) is composed of the CIO, the Deputy Director of IRD, Branch Chief of Operations, DA IT Security Administrator, and the DA Associate Director for Cyber Security.

309.3.2 Incident Coordination Team

The Incident Coordination Team (ICT) is established on an ad hoc basis when the severity of an incident requires coordination with more than one DA Staff Office.

309.3.3 DA Staff Office Directors

DA Staff Office Directors have responsibility for ensuring incidents that occur within systems under their control are handled, responded to, and reported in accordance with the *Computer Incident Reporting Guidelines and Procedures* (under development).

309.4 PROCEDURES

Each SSP must include a section that addresses incident handling, response, and reporting that applies to the particular system under consideration. This section must be consistent with the guidance provided in the *Computer Incident Reporting Guidelines and Procedures* document.

Network scans are conducted on average of every 25 days, but not to exceed every 35 days. The network is scanned after every major configuration change and after every security incident. Scans and results are logged and maintained in the server room. A summary report is given to the ISSPM and to the DA CIO within 5 days of the scan. Scan results include initial scan, corrective actions taken, and validation scan. Network documentation includes a listing and description of known false positives and acceptable risks based on business needs, for comparison to scan results.

309.5 MANAGEMENT CONTROLS

Managers must assure that IRT members at every level understand their responsibilities and the chain of reporting and command when an adverse event occurs. Tests of the response capability should be held regularly and all documentation concerning team members and how to reach them should be kept current.

400 TECHNICAL CONTROLS

Technical Controls consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications. Major categories of technical controls are:

1. Supporting controls, e.g., identification, cryptographic key management, security administration, and system protections
2. Preventive controls, e.g., authentication, authorization, access control enforcement, non-repudiation, protected communications, and transaction privacy.
3. Detection and recovery controls, e.g., audit, intrusion detection and containment, proof of wholeness, restore secure state, and virus detection and eradication.

401 IDENTIFICATION AND AUTHENTICATION

401.1 PURPOSE

DA IT GSSs and MAs must contain technical controls that identify and authenticate users in order to prevent unauthorized access. Control measures will be in accordance with USDA OCIO policies and procedures. The procedures also apply to the use of DA issued wireless, remote, portable, or other similar devices.

401.2 Scope

The identification and authentication guidelines below apply to all DA GSSs and MAs.

401.3 Roles and Responsibilities

401.3.1 CIO

The CIO is responsible for ensuring that all DA GSSs and MAs have documented identification and authentication procedures and that these procedures are in accordance with applicable regulations and guidelines.

401.3.1 DA Staff Office Directors

DA Staff Office Directors are responsible for managing and controlling access to all GSSs and MAs under their control and must ensure that unauthorized persons are prevented from accessing these systems. They must ensure that identification and authentication procedures are utilized and tested, and the results of these tests are reported.

401.4 General Procedures

1. Authentication procedures for the GSS and its MAs should describe how access is controlled and how user authentication is assured. The latter may be through use of password, token, or biometrics.

401.4.1 Documentation

Access control documentation should include a discussion of:

1. How individual accountability and audit trails are implemented;
2. Self-protection techniques for user authentication;
3. Number of invalid access attempts before action is taken and what that action will be;
4. Techniques for limiting access scripts with embedded passwords; and,
5. Any policies for bypassing user authentication requirements, single sign-on, and any compensating controls.

401.4.2 Wireless or Remote Access Devices

DA authentication procedures governing the access of PEDs, and to be used, but that DA is not limited to, are:

1. Personal firewalls and robust authentication methods, (PINS and tokens) will be installed and their use is required on any wireless or remote access device, including laptops and desktop computers, and the peripherals authorized access to the GSS or its MAs.
2. Mutual authentication will be required to gain access to the GSS and its MAs. This requires the acknowledgement of both the client system and the remote access system before their connection can be achieved.
3. Users accessing the GSS or its MAs are to be authorized access only to the file areas they need to accomplish job related tasks.

401.4.3 Password Procedures

Password procedures should follow the NIST guidelines and apply to wireless and remote access devices as well as all directly connected desktop and laptop computers. The following information should be included:

1. Passwords must be at least eight (8) alphanumeric characters;
2. Password characters consist of at least one (1) alpha character, one (1) numeric character, and one (1) special character;
3. Aging time frames and enforcement approach;
4. Number of generations of expired passwords disallowed for use;
5. Procedures for password changes (after expiration, forgotten, or lost);

6. Procedures for handling password compromise; and,
7. Frequency of password changes, how changes are enforced, and who changes passwords should be provided in the procedure.

401.4.3 Digital Signatures and Cryptography

Any use of digital or electronic signatures (including standards used) should be identified. If utilized, digital signatures should conform to FIPS 186-1. If cryptography is employed, key management procedures for key generation, distribution, storage, and disposal should be documented. This also applies to the use of PEDs, wireless and remote access devices, including laptop and desktop computers and their peripherals.

401.5 MANAGEMENT CONTROLS

401.5.1 Access Approval

The Staff Office Director must approve access requests. A record of requests for access and decisions on those requests, including those for wireless and remote access, must be kept on file at the requesting office and the LAN/WAN administrator's office.

401.5.2 Users List

A list of users accessing the system(s) must be established, maintained, and approved. The list will show each user's level of access and the applications they are authorized to access. If possible, the list should indicate a time period for access requirements.

401.5.3 Access List Review

The access listings must be reviewed each month to ensure only authorized users can access the system(s) and to ascertain whether a bona fide need for access still exists.

401 LOGICAL ACCESS CONTROL

402.1 PURPOSE

Logical access is a family of security controls in the technical class dealing with ensuring that logical access controls on the IT system restrict users to authorized transactions and functions. GSSs and MAs should contain system-based mechanisms that control access. The controls must define who is to have access to a specific system resource for the type of transactions and functions they are allowed to perform.

402.2 SCOPE

Logical access controls apply to all GSSs and MAs. They should cover the activities of developers, users, administrators, and the public (if applicable).

402.3 ROLES AND RESPONSIBILITIES

402.3.1 CIO

The CIO is responsible for ensuring that all DA GSSs and MAs have logical access control procedures and that these procedures are in accordance with USDA and DA regulations and guidelines. Approval authority to grant emergency access to systems is vested solely in the CIO.

402.3.2 DA Staff Office Directors

DA Staff Office Directors are responsible for managing and controlling access to all GSSs and MAs under their control. Staff Office Directors ensure that a list of users accessing GSSs and MAs under their control is established and maintained.

402.4 PROCEDURES

402.4.1 General

1. The users of DA issued, as well as those using privately owned devices, must receive special security awareness training related to security issues related to the use of wireless or remote access device, including laptops and desktop computers, and their peripherals.
2. During the training, the user will be informed that their device(s) is subject to periodic security screenings for appropriate configurations, the presence of viruses, the installation of antivirus protection, patch levels, and equipment to be sure they are up-to-date as required by the Configuration Management Plan. If evidence of the illegal use of the device(s) during official business hours is found as a result of the screening, the device may be seized.
3. In accordance with the "Personal Use Policy," all users be made aware of the fact that they have no expectation of privacy related to the use of the device(s) with the exception that, for privately owned devices, where this restriction is only during duty hours.
4. All users can expect periodic security checks to ensure conformance with current DA standards.
5. The information in 1 through 3 above must be confirmed in writing as being understood and signed by the user after the appropriate training is received.
6. The signed document must accompany and be filed with the application for remote access for approval by the CIO

402.4.2 For DA Personnel and Contractors

The following access control measures apply to DA personnel and contractor hired personnel authorized access to the GSS and Its MAs.

1. Though access to the GSS and its MAs is normally done using USDA & DA issued remote access devices, users desiring to access them using privately owned wireless and remote access devices including laptop and desktop computers, or similar device(s), either within a USDA controlled facility, telecommuting/flexiplace facility, or other location must receive approval from the DA CIO.
2. Authorized users of DA issued or privately owned wireless or remote access devices, including laptop and desktop computers and their peripherals, may only access the GSS and its MAs during the times authorized by the DA CIO.
3. Controls should be in place to authorize or restrict the activities of users and system personnel within the system. Hardware or software features that are designed to permit only authorized access to the application or within the application, to restrict users to authorized transactions and functions, should be described.
4. Application users, including those authorized to access an application using a wireless, remote, portable, or similar device, should be restricted from accessing the operating system, other applications, or any system resources not needed in the performance of their duties. The discussion should describe how access rights are granted and whether a job function is used to assign privileges.
5. Security profiles should be established to specifically address the access rights of wireless, remote, portable, or similar device, their authorized time-of-day usage, and their server and service access.
6. The system should be able to detect unauthorized transaction attempts by both authorized and/or unauthorized users.
7. Access to GSS(s) and MA(s) after hours or on weekends should be restricted. Procedures for implementing such restrictions should be documented.
8. Systems should automatically blank screens and/or disconnect users after an established period of user inactivity. Disconnected users should be required to enter a unique password before being reconnected to the system.
9. A list of users accessing the system(s) must be established, maintained, and approved. The list will show each user's level of access and the applications that they are authorized to access. If possible, the list should indicate a time period for access requirements. The CIO shall verify the access listings on a regular basis to ensure that only authorized users can access the system(s), this includes former employees;
10. A separate list of users accessing the system(s) using a DA issued wireless, remote, portable, or other similar device must be established, maintained, and approved. The list will show each user's level of access and the applications that they are authorized to access. If possible, the list should indicate a more restrictive time period than item 6, above, for access requirements. The access listings must be validated on a regular basis to ensure that only authorized users can remotely access the system(s);
11. A list of persons authorized to access each GSS and MA during an emergency will be established. The CIO will approve this list, in writing.

12. Default or vendor-supplied passwords will be de-activated immediately upon installation of hardware, software, firmware, or an application.
13. IT system software must be able to correlate system activity to the user causing the activity.
14. For systems where encryption is required, the process for interacting with the access control procedures should be documented.
15. The use of warning banners should be considered. If warning banners are used, an example should be provided in the documentation along with an indication that, if appropriate, the language has been approved by the Department of Justice, Computer Crime, and Intellectual Properties Section.
16. A password will be required to "boot up" any DA issued wireless or remote access device, including laptop and desktop computers. If the unit has the capability of securing its hard drive(s) with a password, this feature will be activated.
17. User of a DA issued wireless or remote access device, including a laptop or desk top computer, will be required to enter a password prior to logging onto LAN resources.
18. The mechanisms used to manage access should be fully documented in the SSP of each GSS and MA.

402.4.3 Privately Owned Wireless and Remote Device Access

After determining that access to the GSS or its MAs is needed to meet job demands, the DA CIO may authorize DA, and DA contract employees, access to the GSS or its MAs using their own wireless or remote access device, including laptops and desktop computers, and their peripherals. This authorization may be provided after the DA CIO receives assurance that:

1. The person requesting to use a privately owned device(s) to connect to the GSS and/or its MA resources must complete the required request for such use and meets the same criteria as those used for organizationally issued devices.
2. The privately owned device(s) meet the same hardware and software functionality and performance standards as organizationally issued devices.
3. The privately owned device(s) have been checked and validated by IT security personnel prior to being authorized connection to the GSS and/or its MAs.
4. The security requirements for the use of privately owned devices are to be the same as those for the DA issued devices.

402.4.4 Public Access

If public access is provided by an IT system, additional security controls may be required to protect the integrity of the application and the confidence of the public in the application. The following should be considered:

1. Public identification and authentication;

2. Access controls that limit what users read, write, modify, or delete;
3. Alternate methods of distribution;
4. Prohibiting public access to live databases;
5. Audit trails;
6. User confidentiality;
7. System and data availability; and
8. Legal concerns.

402.5 MANAGEMENT CONTROLS

The use of an access control list (ACL) is a primary management tool in the implementation of logical access controls. An ACL should be developed, maintained, and, documented. The ability to detect unauthorized activities (through ACLs) should also be discussed, if present.

Procedures have to be implemented, documented, and tested. Test results may require revisions to procedures. If so, procedure documentation should be updated accordingly.

403 AUDITS TRAILS

403.1 PURPOSE

Audit trails maintain records of system activity for GSSs and MAs. Properly collected and maintained, audit trails support reconstruction of security incidents, tracking of individual actions, and problem investigation. Each DA Staff Office, division, and unit is responsible for establishing and maintaining records of IT system security audits and audit trails sufficient to reconstruct any relevant security event. This section provides guidance on the development and administration of an audit trail.

403.2 SCOPE

Audit trails are applicable to all GSSs and MAs utilized within DA. New systems are required to include a section on audit and audit trails in their SSPs. Existing systems are required to review (and update if necessary) the audit and audit trail logs in SSPs annually.

403.3 ROLES AND RESPONSIBILITIES

403.3.1 CIO

The CIO is responsible for verifying that audit trails are being kept and that audit trail logs are secured.

403.3.2 DA Staff Office Directors

DA Staff Office Directors are responsible for ensuring that audit trails are implemented for all GSSs and MAs under their control. They are responsible for ensuring that the audit trail administrator is not the same person who administers the access control function for the GSS or MA.

403.4 PROCEDURES

An audit trail program is developed to include data collection, review, and reporting. For all new systems, the SSP must contain a section describing the audit procedures, the audit trail, and the mechanisms for managing the audit information. The audit trail captures and records IT system actions and provides reports concerning access to and actions against IT systems. Audit trail logs must be secured to prevent unauthorized access and modification and must be in sufficient detail to enable the reconstruction of a security event.

403.4.1 Data Elements Collected

The audit trail procedure must describe the systems that are covered, the data elements that will be collected and maintained, how and under what circumstances these elements will be collected, and any special circumstances that will prevail. Data stored in audit trails must be protected against modification. Coverage must be described and be extended to all users including System Managers and System Administrators. The following items comprise a minimum list of data elements to be collected:

1. System name,
2. User identification,
3. Workstation/terminal identification,
4. Date and time of entry,
5. Date and time of exit,
6. System segment accessed, and
7. Activities performed.

403.4.2 Remote Keystroke Monitoring

Remote monitoring replicates the action of a user. A special circumstance occurs if keystroke monitoring is being implemented. Keystroke monitoring records keystrokes entered by a user and the computer’s response. If keystroke monitoring is in effect, users must be notified on at least a monthly basis that keystrokes are being monitored.

403.4.3 Remote Access

The data elements collected for the audit trail should be augmented for users that access systems remotely (Web, FTP, or telnet) using wireless, remote, portable, or other similar devices. These include tracking attempted log-ins with erroneous passwords, multiple erroneous passwords, and other evidence of potential intruder attacks.

403.4.4 Collection Process

1. The audit procedure must address software used for data collection on each of the major components of the system. This information should be consistent with the SSP for each GSS or MA, which contains information on how audit trails are being implemented.

2. An audit information collection process should be established. This process must include backup procedures for the audit trail logs. For instance, audit logs can be removed from the system after a shift, daily, or at some intermediate interval. Daily collection is recommended.

3. Automated tools exist to serve in analysis of audit trails or to enable audit records to be reduced in size while preserving detail. The SSP should indicate whether such tools are being used. If they are, procedures for using them should be included in the audit procedure.

403.5 Reviews of Audit Trail Logs

403.5.1 Regular Reviews

The audit procedure should include a regular review cycle for the audit trail logs. If the logs of the system are of a sensitive or critical nature, frequent review should be considered. Dates for audit trail reviews should not be published.

403.5.2 Ad Hoc Reviews

The audit procedure should specify the circumstances under which an ad hoc review is required or prudent. Ad hoc reviews should be performed after suspect events have occurred. If the breach was particularly serious, the audit logs should be reviewed more frequently.

403.5.3 Post-Incident Reviews

Any security breach, event, or incident involving a system should trigger a review of audit trail logs once the problem has been resolved. Data collection practices should be modified at this time if warranted.

403.5.4 Spot Reviews

Spot reviews of the audit trail logs are optional and may be indicated if the system has security problems. As a general rule, an increase in incidents should trigger an increase in monitoring of the audit trail logs.

403.5.5 Review of Authorized User Audit Records

Security problems frequently arise with disgruntled individuals or individuals who are no longer using the system but whose access authorizations have not been removed. The audit procedure should address this threat specifically. A list of the names of employees and contractors who are no longer working on the systems should be maintained. A regular review of the audit trails should be scheduled to assure that only authorized users are accessing the systems. During a period when there is a large turnover of personnel (federal or contractor) or when a security incident has occurred, this review should be scheduled at a weekly interval until the situation stabilizes.

403.5.6 General Review Guidance

Guidelines and schedules for the review of audit logs are documented in the SSP and are a critical part of the audit procedure. The procedure should provide for review of the audit logs using these guidelines and schedules. Any discrepancies or problems are reviewed with other relevant personnel. For example, an incidence of a user ID for an individual whose access should have been terminated is reviewed with the system access administrator. Audit logs are reviewed regularly as part of the annual security audit. They are also subject to random review by authorized internal and external personnel. The review guidelines should be evaluated annually to determine whether any changes should be made.

403.5.7 Analysis of the Audit Trail

When the audit trail is undergoing a regularly scheduled review (e.g. a review not triggered by an incident), the following should be considered:

1. Any access by user ids that are no longer valid;
2. Workstations or user IDs that remain logged on with long periods of inactivity, especially during a lunch break;
3. User access on multiple workstations;
4. Multiple user access on a single workstation;
5. Invalid attempts to access system software or sensitive files; and
6. Patterns of usage.

403.5.8 Random Samples

A random sample of user IDs should be selected for a more detailed analysis as part of the regularly scheduled review.

403.5.9 On-Line Monitoring

On-line monitoring of the audit trail is recommended. In addition, a series of reports should be available. Standard queries and reports should provide information by all of the data elements.

403.5.10 Action Reports

The audit procedure should address actions to be taken after an incident has occurred (security breach, system problem, user problem). At this time, a special review is conducted and the procedures found in the USDA *Computer Incident Reporting Guidelines and Procedures* are followed.

403.6 MANAGEMENT CONTROLS

The following management controls provide a minimum level to assure the appropriate use and recording of audit records. Each DA GSS and MA should establish the controls needed to ensure the appropriate handling, retention, storage, and destruction of audit records. The controls are:

1. Access to all audit trail logs should be limited, the audit trail should be password-protected, and should be stored at a location separate from the system being tracked.

2. DA policy dictates that audit logs be kept as required by law. After a log has been reviewed, it can be retired to the offline storage. The offline log should be purged monthly, after the entry of a new month's information. The exception to this guideline occurs when there is a security event requiring analysis.

3. A special case of record retention occurs when the audit trail is related to a security event and is required for legal purposes. In this case, the log should be preserved in a secure, tamper-proof file until the legal matter is resolved. It is recommended that this log be transferred to a separate location and a copy retained in the audit trail log.

4. SSPs should contain information as to where the on-line and off-line logs are stored.

APPENDIX A, REFERENCES

USDA DA Information Technology Security Policy Manual, draft December 10, 2001.

NIST 800-18 Guide for Developing Security Plans for Information Technology Systems.

NIST 800-37 Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems.

NIST 800-46, Security for Telecommuting and Broadband Communications

Federal Information Security Management Act (FISMA) (e-Government) (P.L. 107-347), which includes Title III of 2002.

Federal Information Security Management Act passed in 2002 as part of the E-Government Act. Public Law 107-347.

OMB Circular A-123, “Management Accountability and Control.”

OMB Circular A-130, “Management of Federal Information Resources.”

OMB Memorandum, 01-08, “Guidance on Implementing the Government Information Security Reform Act”

USDA DM-3500-001, USDA Computer Incident Response Procedures Manual.

OCS CS-009 “Interim Guidance on USDA Configuration Management, Par 1 – Policy and Responsibilities”

OCS CS-019 “Privacy Requirements” and “Privacy Impact Questionnaire.”

OCS CS-028 “IT Contingency and Disaster Planning.”

APPENDIX B, TERMS AND DEFINITIONS

Access
The opportunity to make use of an information system (IS) resource.

Access Control
The limiting access to information system resources to authorized users, program, processes, and controls.

Accountability
The principle that responsibilities for ownership and/or oversight of IS resources are explicitly assigned and that assignees are answerable to proper authorities for the stewardship of resources under their control.

Agency
A federal department, major organizational unit in a department, or independent agency

Application
A software package designed to perform a specific set of functions, such as word processing, or communications. See also **program.**

Attack
An intentional attempt to bypass the physical or information security measures and controls protecting an IS.

Audit
An independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established security policies and procedures, and/or to recommend necessary changes in controls, policies, or procedures to meet security objectives.

Audit Trail
A chronological record of system activities or message routing that permits reconstruction and examination of a sequence of events.

Authentication
A security measure designed to measure the validity of a transmission, message, or originator; or as a means of verifying a user's authorization to access specific types of information.

Banner
A display on an IS that sets forth conditions and restrictions on a system and/or data use.

Confidentiality
An assurance that information is not disclosed to unauthorized persons, processes, or devices.

APPENDIX B, TERMS AND DEFINITIONS (Continued)

Configuration Management The management of security features and assurances through control of changes made to hardware, software, firmware, documentation, tests, test fixtures, and test documentation throughout the life cycle of an IS.

Contingency Plan A plan maintained for emergency response, backup operations, and post-disaster recovery of an IS, to ensure availability of critical resources and facilitate the continuity of operations in an emergency.

Cryptography The science of encrypting (coding) plain data and information into a form intelligible only to authorized persons who are able to decrypt (decode) it.

Data Integrity A condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

Disaster Recovery A plan describing the process of restoring an IS to full operation after an interruption in service, including equipment repair/replacement, file recovery/restoration and the resumption of service to users. (Also known as Business Resumption)

Disaster Recovery Plan The plan used to guide an organization’s disaster recovery effort.

Disaster Recovery Team The group of persons, selected for their specific skills, that are used to execute a Disaster Recovery Plan

E-mail The abbreviation for electronic mail, which consists of messages sent over an IS by communications applications. E-mail that is sent from one computer system to another or over the Internet must pass through gateways to leave the originating system and to enter the receiving system.

Environment The total of the external procedures, conditions, and objects affecting the development, operation, and maintenance of an IS.

Federal Computer Incident Response Capability The U.S. Government’s focal point for handling computer security related incidents.

APPENDIX B, TERMS AND DEFINITIONS (Continued)

Firmware
An application recorded in permanent or semi-permanent computer memory.

Gateway
An interface between networks that facilitates compatibility by adapting transmission speeds, protocols, codes, or security measures.

General Support System
An interconnected set of information resources under the same direct management control which shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization.

Incident
An occurrence that has been assessed as having an adverse effect on the security or performance of an IS.

Incident Recovery Team
The group of persons, selected for their specific skills that are used to correct the effects of an IT incident.

Information Systems
All the electronic and human components involved in the collection, processing, storage, transmission, display, dissemination, and disposition of information. An IS may be automated (e.g., a computerized IS) or manual (e.g., papers in a file).

Information Systems Security
The measures and controls that ensure confidentiality, integrity, and availability of IS assets including hardware, software, firmware, and information being processed, stored, and communicated. This is also called computer security.

Information System Security Officer
The person assigned to implement an organization's information system security policy.

Information Technology Security Administrator
The person assigned to manage an organization's information system security program.

APPENDIX B, TERMS AND DEFINITIONS (Continued)

Information Technology Security Officer

The person assigned to coordinate the development and and implementation of an organization's information technology security policies and procedures.

Integrity

The condition existing when an IS operates without unauthorized modification, alteration, impairment, or destruction of any of its components.

Interface

A common boundary or connector between two applications or devices, such as a graphical user interface (GUI) that allows a user to interact with an application written in code.

Intrusion

Attacks or attempted attacks from outside the security perimeter of an IS.

Laptop Computer

A portable computer usually powered by a rechargeable battery. The smaller versions are also called notebook computers.

Major Application

An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

Local programs designed to meet particular office and standard commercial off-the-shelf software (such as word processing software, electronic mail software, utility software, or other general- purpose software) are generally not considered major applications and would usually be covered by the security policies and procedures for the general support system on which they are installed. Certain of these applications, however, because of the sensitive information in them, require special management oversight and should be treated as major.

National Information Protection Center

The U.S. Government's focal point for threat assessment, warning, investigation, and response for threats or attacks on its critical infrastructures.

APPENDIX B, TERMS AND DEFINITIONS (Continued)

Network Security

The security procedures and controls that protect a network from: (1) unauthorized access, modification, and information disclosure; and (2) physical impairment or destruction.

Non-repudiation

A cryptographic service that legally prevents the originator of a message from denying authorship at a later date.

Operating system

The software required by every computer that: (1) enables it to perform its basic tasks such as controlling disks, drives, and peripheral devices; and (2) provides a platform on which applications can operate.

Operational Controls

The security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).

Password

A string of characters containing letters, numbers, or other keyboard symbols that is used to authenticate a user's identity or authorize access to data. Only the authorized user who originated it generally knows the password.

Policy

A document that delineates the security management structure, clearly assigns security responsibilities, and lays the foundation necessary to reliably measure progress and compliance.

Personal Digital Assistant (PDA)

A handheld computer that serves as an organizer for personal information. It generally includes at least a name and address database, a To Do List and a note taker. The unit may include a small on-screen keyboard that is tapped with a pen. Data is synchronized between a user's PDA and desktop computer by cable or wireless transmission.

APPENDIX B, TERMS AND DEFINITIONS (Continued)

Portable Electronic Device) (PED)

Any electronic device that is capable of receiving, storing or transmitting information using any format (i.e., radio, infrared, network or similar connections) without permanent connections to Federal networks.

Portable Storage Device

Any electronic device that is capable of storing information in a form that allows it to be physically moved from one location to another, such as, ZIP Drives, floppy, CD, and DVD disks, flash memory cards, and other similar devices.

Procedures

A document that focuses on the security control areas and management's position.

Program

Sets of instructions in code that, when executed, cause a computer to perform a task.

Remote Access Device

A hand held or larger device that may upload, download, or remotely access information in the DA GSS and/or its MAs. These include but are not limited to laptop and notebook computers, cellular phones that may transmit data or e-mail, Personal Data Access (PDA) devices, wireless access devices, portable storage drives, etc., and desktop computers remotely accessing the GSS and its MAs.

Risk

The possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

Risk Management

The ongoing process of assessing the risk to automated information resources and information. Part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

Rules of Behavior

The rules that are established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of portable storage devices, use of copyrighted works, unofficial use of

APPENDIX B, TERMS AND DEFINITIONS (Continued)

federal government equipment, assignment, and limitation of system privileges, and individual accountability.

Sensitive Information Unclassified information, the loss, misuse, or unauthorized disclosure of which could adversely affect the national security interest, the conduct of federal programs, or the privacy of individuals protected by the Privacy Act (5 U.S.C. Section 552a). Information systems containing sensitive information are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L. 100-230). (This information is also called Sensitive but Unclassified **(SBU)**.

Software The electronically stored commands and instructions that make an IS functional, including the operating system, applications, and communications protocols.

System Administrator (SA) The person responsible for the effective operation and maintenance of an IS, including the implementation of standard procedures and controls to enforce an organization's security policy.

System Integrity Optimal functioning of an IS, free from unauthorized impairment or manipulation.

System of Records The Privacy Act of 1974 (Privacy Act), as amended, applies to a record about an individual that is maintained in a system of records from which information is retrieved by a unique identifier associated with each individual, such as a name or social security number. The information about each individual is called a ``record" and the system, whether manual or computer-driven, is called a ``system of records." The Privacy Act requires each agency to publish notices of systems of records in the Federal Register and to prepare reports to the Office of Management and Budget (OMB) whenever the agency publishes a new or ``altered" system of records.

System Security Plan A formal document listing the tasks necessary to meet system security requirements, a schedule for their accomplishment, and where the responsibilities for each task are assigned.

Vulnerability

A flaw in security procedures, software, internal system controls or implementation of an IS that may affect the integrity, confidentiality, accountability, and/or availability of data or services. Vulnerabilities include flaws that may be deliberately exploited and those that may cause failure due to inadvertent human actions or natural disasters.

APPENDIX C, ACRONYMS

ACL	Access Control List
ATA	Audit Trail Administrators
C&A	Certification and Accreditation
C-DRP	Contingency-Disaster Recovery Plans
CIO	Chief Information Officer
CM	Configuration Management
CO	Certifying Official
CSH	Computer Security Handbook
DAA	Designated Approving Authority
DOJ	Department of Justice
GAO	General Accounting Office
GSA	General Services Administration
GSS	General Support Systems
GUI	Graphical User Interface
HVAC	Heating, Ventilation, and Air Conditioning
IATO	Interim Authority to Operate
ID	Identification
IG	Inspector General
ICT	Incident Coordination Team
IRM	Information Resources Management
IRT	Incident Response Team
IS	Information System
ISSO	Information System Security Officers
ITSA	Information Technology Security Administrator
ITSO	Information Technology Security Officer
IT	Information Technology
ITS	Information Technology Security
ITSA	Information Technology Security Administrator
ITSO	Information Technology Security Officer

APPENDIX C, ACRONYMS (Continued)

OCIO	Office of the Chief Information Officer
OCS	Office of Cyber Security
OTIS	Office of Technology and Information Services
PD	Position Descriptions
PDA	Personal Digital Assistant
PED	Portable Electronic Device
RTM	Requirements Traceability Matrix
SBU	Sensitive But Unclassified
SM	System Managers
SPP	Security Program Plan
SSAA	System Security Authorization Agreement
SSP	System Security Plan
UPS	Uninterruptible Power Sources
USDA	Department of Agriculture

APPENDIX D, DA PATCH UPDATE PROCEDURES AND CHECKLIST

Patch Update Procedures

DA has implemented a Patch Link tool and service to support the GSS network environment. The network engineers for review maintain a DA Patch Update Checklist at any time. The procedures include:

1. Review new patches provided from Patch Link to assess if needed in DA's computing environment. DA engineers must ensure that the patches are tested and certified by the Patch Link service prior to deployment.
2. The CIO must grant permission before any patches can be scheduled or deployed to the GSS for pushing to the computers on the DA network.
3. The new patch must be added to the computer patch baseline for new PC connecting to the network so that all patches will be deployed to the new PC.

Attached is a DA Patch Update Checklist used by the network engineers when new patches are provided by the Patch Link services. This checklist must be maintained in a binder in the computer room and used each time a patch is entered into the computer baseline.

APPENDIX D, DA PATCH UPDATE PROCEDURES AND CHECKLIST (Continued)

DA PATCH UPDATE CHECKLIST

Engineer Name: Date:

REVIEW:	**Response**	**Comments**
What is the patch for?		
How Critical is it?		
Is the patch certified by PatchLink?	Yes No	
Where does it need to Be deployed?		
When can it be Deployed?		
How will it be deployed?		
Deployment:		
Request permission from DA CIO to push patch. (who approved)		
Schedule a date to deploy. (enter scheduled date)		
Date deployed. (enter date deployed)		
Verify good deployment	Yes No	
Identify if cleanup needed and why?	Yes No	
Schedule cleanup (enter scheduled date)		
Verify cleanup	Yes No	
PATCH BASELINE:		
Update computer baseline		
Successful	Yes No	

APPENDIX E, REGISTERING AND CERTIFYING USER SYSTEMS

STANDARD DESKTOP CONFIGURATION

SOFTWARE ON ALL DESKTOPS

Microsoft Windows 2000 with current Service Pack (SP4)
Or Window XP SP1 with Office XP Professional

Microsoft Office 2000 or XP Professional
- Access
- Excel
- Outlook
- PowerPoint
- Word

Adobe 6.0
CENS 3.1
Symantec 8.1
WinZip 8.1

SOFTWARE ON ALL OCFO DESKTOPS, SOME DA DESKTOPS

Word Perfect 11
Lotus 1-2-3 v 9.8
TN3270 Plus (Connections to NFC and NITC)
NFC Logon
Informs 4.3
Secure Remote 5.5 (Connections to Brio, NFC, and School St.)
Brio 6.6 Insight or Explorer (not on image, will install as needed, with appropriate level)

OTHER SOFTWARE LOADED FROM NETWORK

SMS to be loaded via network
Patchlink to be pushed to clients

OTHER STANDARDS

Computer Naming convention (building room# username)
Power User rights (not Administrator) for user
Administrator password Naming convention
Member of DA domain
Symantec in managed mode and pointed to DA-south-dc
Patch link started
H and share drives in My Computer

APPENDIX E, REGISTERING AND CERTIFYING USER SYSTEMS (Continued)

INFORMATION FOR CERTIFICATION AND REGISTRATION

1. Employee ID;
2. Staff Office name;
3. Contact name;
4. Contact title;
5. Office location;
6. Contract phone number;
7. Assignee name;
8. Assignee room number;
9. Assignee phone number;
10. Employer;
11. Contractor name;
12. PC name;
13. Description of computer;
14. Serial number;
15. Manufacturer;
16. Registration date;
17. Last update date;
18. MAC address;
19. If scanned;
20. If cleaned;
21. If anti virus loaded;
22. If patch link added;
23. If added to domain; and
24. If remote user.

APPENDIX E, REGISTERING AND CERTIFYING USER SYSTEMS (Continued)

PROCEDURES FOR CERTIFYING AND REGISTERING REMOTE COMPUTERS

The following procedures are used to certify and register computers that access DA's GSS remotely:

1. Notify remote users to bring in laptops and desktop computers for certification and registration.

2. Schedule users for certification and registration.

3. Test machine for the latest patches or critical updates.
 update machine if needed.

4. Verify DA standard configuration.

5. Scan machine for viruses.

6. Check machine for latest virus software and definitions.
 update machine if needed.

7. Register machine by completing the DA IRD certify and register web site.

8. Return to user.